Skript zur Vorlesung

Angewandte Diskrete Mathematik

Wintersemester 2009/10

Prof. Dr. Helmut Maier
Dipl.-Math. Hans- Peter Reck

Institut für Zahlentheorie und Wahrscheinlichkeitstheorie
Universität Ulm

Inhaltsverzeichnis

Kapitel 1

Teilbarkeit

1.1 Teilbarkeit ganzer Zahlen

Definition 1.1.1. Eine ganze Zahl b heißt durch eine ganze Zahl $a \neq 0$ teilbar, falls es ein $x \in \mathbb{Z}$ gibt, so daß $b = ax$ ist, und wir schreiben $a|b$. Man nennt a einen Teiler von b, und b heißt Vielfaches von a. Falls b nicht durch a teilbar ist, schreiben wir $a \not| b$.

Satz 1.1.2.

(a) $a|b \Rightarrow a|bc$ *für alle* $c \in \mathbb{Z}$

(b) $a|b$ *und* $b|c \Rightarrow a|c$

(c) $a|b$ *und* $a|c \Rightarrow a|(bx + cy)$ *für alle* $x, y \in \mathbb{Z}$

(d) $a|b$ *und* $b|a \Rightarrow a = \pm b$

(e) $a|b$ *und* $a, b > 0 \Rightarrow a \leq b$

(f) *Ist* $m \neq 0$*, dann gilt:* $a|b \Leftrightarrow ma|mb$.

1.2 Eindeutigkeit der Primfaktorzerlegung

Definition 1.2.1. Eine natürliche Zahl $p \in \mathbb{N}$ heißt Primzahl, wenn p nur die positiven Teiler 1 und p besitzt.

Beispiel 1.2.2. Es ist $n = 91$ keine Primzahl, da $91 = 7 \cdot 13$ gilt.
Dafür ist $p = 17$ eine Primzahl.

Definition 1.2.3. Unter der (kanonischen) Primfaktorzerlegung einer natürlichen Zahl $n > 1$ versteht man eine Darstellung der Gestalt $n = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$ mit $p_1 < \ldots < p_r$ und $\gamma_i \in \mathbb{N}$ für $i = 1, \ldots, r$.

Beispiel 1.2.4. Die Zahl $n = 9000$ besitzt die kanonische Primfaktorzerlegung $9000 = 2^3 \cdot 3^2 \cdot 5^3$.

Satz 1.2.5. *(Fundamentalsatz der Arithmetik)*
Die kanonische Primfaktorzerlegung einer natürlichen Zahl $n > 1$ *existiert stets und ist eindeutig.*

1.3 Berechnung von ggT und kgV anhand der Primfaktorzerlegung

Definition 1.3.1. Es seien $a, b \in \mathbb{Z}$, nicht beide gleich 0.
Der größte gemeinsame Teiler von a und b, $ggt(a, b)$, ist die größte positive ganze Zahl d, für die gilt: $d|a$ und $d|b$.
Es sei nun $a \neq 0$ und $b \neq 0$.
Das kleinste gemeinsame Vielfache von a und b, $kgV(a, b)$, ist die kleinste positive Zahl V, für die gilt: $a|V$ und $b|V$.

Satz 1.3.2. *Es seien* $m = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$ *und* $n = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$ *mit* p_i *verschiedene Primzahlen,* $\alpha_i, \beta_i \in \mathbb{Z}$, $\alpha_i \geq 0$ *und* $\beta_i \geq 0$.
Dann ist

$$\begin{aligned} ggT(m,n) &= p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r} \\ kgV(m,n) &= p_1^{\delta_1} \cdot \ldots \cdot p_r^{\delta_r} \end{aligned}$$

mit $\gamma_i = \min(\alpha_i, \beta_i)$ *und* $\delta_i = \max(\alpha_i, \beta_i)$.

Bemerkung 1.3.3. Die obige Darstellungen stellen nicht unbedingt die kanonische Primfaktorzerlegung von m und n im Sinne von Definition 1.2.3 dar, bei der alle Exponenten positiv sein müssen. In manchen Fällen ist es nötig, Potenzen p_i^0 einzufügen, um zu gewährleisten, daß die in beiden Produkten vorkommenden Primzahlen dieselben sind.

Beispiel 1.3.4. Es sei

$$\begin{array}{lllllll} m = 90090 & = 2 & \cdot 3^2 & \cdot 5 & \cdot 7 & \cdot 11 & \cdot 13 \\ n = 2300 & = 2^2 & & \cdot 5^2 & & & \cdot 23 \end{array}$$

Bestimme $ggT(m, n)$ und $kgV(m, n)$.

Lösung:
Wir schreiben m und n so als Produkte, daß die in ihnen vorkommenden Primzahlen dieselben sind:

$$\begin{array}{lllllllll} m = 90090 & = 2^1 & \cdot 3^2 & \cdot 5^1 & \cdot 7^1 & \cdot 11^1 & \cdot 13^1 & \cdot 23^0 \\ n = 2300 & = 2^2 & \cdot 3^0 & \cdot 5^2 & \cdot 7^0 & \cdot 11^0 & \cdot 13^0 & \cdot 23^1 \end{array}$$

Nach Satz 1.3.2 ist

$$\begin{array}{lllllllll} ggT(m,n) & = 2^1 & \cdot 3^0 & \cdot 5^1 & \cdot 7^0 & \cdot 11^0 & \cdot 13^0 & \cdot 23^0 & = 10 \\ kgV(m,n) & = 2^2 & \cdot 3^2 & \cdot 5^2 & \cdot 7^1 & \cdot 11^1 & \cdot 13^1 & \cdot 23^1 & = 20720700 \end{array}$$

1.4 Der Euklidische Algorithmus

Der ggT zweier natürlicher Zahlen m und n kann mittels des Euklidischen Algorithmus bestimmt werden. Dieser besteht in einer wiederholten Anwendung der Division mit Rest.

Satz 1.4.1. *(Division mit Rest)*
Es seien $a \in \mathbb{Z}$ *und* $b \in \mathbb{N}$.
Dann gibt es $q \in \mathbb{N}_0$, *so daß* $a = q \cdot b + r$ *mit* $0 \leq r < b$.
Es ist $b|a$ *genau dann, wenn* $r = 0$ *ist.*
Man nennt q *auch den Quotienten und* r *den Rest der Division durch* b.
Wir sagen auch: a *läßt bei Division durch* b *den Rest* r.

Beispiel 1.4.2. Für $a = 17$ und $b = 5$ erhalten wir: $17 = 3 \cdot 5 + 2$, also $q = 3$ und $r = 2$.
Die Zahl 17 läßt also bei Division durch 5 den Rest 2.

Satz 1.4.3. *(Euklidischer Algorithmus)*
Es seien $a, b \in \mathbb{Z}$, $b > 0$.
Durch wiederholte Anwendung der Division mit Rest erhält man eine Reihe von Gleichungen:

$$\begin{aligned} a &= q_1 \cdot b + r_1, \quad 0 \leq r_1 < b \\ b &= q_2 \cdot r_1 + r_2, \quad 0 \leq r_2 < r_1 \\ r_1 &= q_3 \cdot r_2 + r_3, \quad 0 \leq r_3 < r_2 \\ &\vdots \quad\quad \vdots \\ r_{n-2} &= q_n \cdot r_{n-1} + r_n, \quad 0 \leq r_n < r_{n-1} \\ r_{n-1} &= q_{n+1} \cdot r_n \end{aligned}$$

Dann ist r_n, also der letzte von 0 verschiedene Rest, der größte gemeinsame Teiler von a und b: $r_n = ggT(a, b)$.
Durch sukzessives Auflösen der obigen Gleichungen nach r_i läßt sich r_n als ganzzahlige Linearkombination von a und b ausdrücken: $r_n = ax + by$ mit $x, y \in \mathbb{Z}$.

Eng mit dem Euklidischen Algorithmus ist die Theorie der linearen Diophantischen Gleichungen verbunden. Der Begriff Diophantische Gleichung bezieht sich nicht auf die Form der Gleichung, sondern auf die Fragestellung: man interessiert sich nur für ganzzahlige Lösungen. Eine lineare Diophantische Gleichung ist eine der Gestalt $ax + by = c$ mit $a, b, c \in \mathbb{Z}$.

Satz 1.4.4. *Es seien $a, b, c \in \mathbb{Z}$ und a, b nicht beide gleich 0.*
Die lineare Diophantische Gleichung $ax + by = c$ ist genau dann lösbar, wenn $ggT(a, b)|c$.
Eine Lösung kann gefunden werden, indem man die Gleichung $ax + by = d$ mit $d = ggT(a, b)$ mit dem Euklidischen Algorithmus löst und die Lösung mit $\frac{c}{d}$ multipliziert.

Beispiel 1.4.5. Man bestimme den ggT von $a = 294$ und $b = 201$ und drücke ihn als ganzzahlige Linearkombination von a und b aus.

Lösung:
Der Euklidische Algorithmus ergibt:

$$\begin{aligned} 294 &= 201 + 93 \\ 201 &= 2 \cdot 93 + 15 \\ 93 &= 6 \cdot 15 + 3 \\ 15 &= 5 \cdot 3 \end{aligned}$$

Also ist $ggT(294, 201) = 3$.
Die Linearkombination wird durch sukzessive (rückwärtige) Auflösung der Gleichungskette erhalten:

$$\begin{aligned} 3 &= 93 - 6 \cdot 15 = 93 - 6 \cdot (201 - 2 \cdot 93) \\ &= 13 \cdot 93 - 6 \cdot 201 = 13 \cdot (294 - 201) - 6 \cdot 201 \\ &= 13 \cdot 294 - 19 \cdot 201 \end{aligned}$$

Eine Lösung der Diophantischen Gleichung $294x + 201y = 3$ ist also $x = 13$ und $y = -19$.

Beispiel 1.4.6. Finde eine Lösung der Diophantischen Gleichung $73685x + 25513y = 10$ oder zeige, daß sie unlösbar ist.

Lösung:
Der Euklidische Algorithmus ergibt:

$$\begin{aligned}
73685 &= 2 \cdot 25513 + 22659 \\
25513 &= 1 \cdot 22659 + 2854 \\
22659 &= 7 \cdot 2854 + 2681 \\
2854 &= 1 \cdot 2681 + 173 \\
2681 &= 15 \cdot 173 + 86 \\
173 &= 2 \cdot 86 + 1 \\
86 &= 86 \cdot 1
\end{aligned}$$

Also ist $ggT(73685, 25513) = 1$.

Wir lösen nun zunächst die Gleichung $73685x' + 25513y' = 1$:

$$\begin{aligned}
1 &= 173 - 2 \cdot 86 = 173 - 2 \cdot (2681 - 15 \cdot 173) \\
&= 31 \cdot 173 - 2 \cdot 2681 = 31 \cdot (2854 - 2681) - 2 \cdot 2681 \\
&= -33 \cdot 2681 + 31 \cdot 2854 = 31 \cdot 2854 - 33 \cdot (22659 - 7 \cdot 2854) \\
&= 262 \cdot 2854 - 33 \cdot 22659 = 262 \cdot (25513 - 22659) - 33 \cdot 22659 \\
&= -295 \cdot 22659 + 262 \cdot 25513 = -295 \cdot (73685 - 2 \cdot 25513) + 262 \cdot 25513 \\
&= -295 \cdot 73685 + 852 \cdot 25513
\end{aligned}$$

Die Diophantische Gleichung $73685x' + 25513y' = 1$ hat also die Lösung $x' = -295$ und $y' = 852$.
Eine Lösung von $73685x + 25513y = 10$ ergibt sich daraus durch Multiplikation mit 10:
$x = -2950$ und $y = 8520$.

In einer tabellarischen Darstellung sieht die Lösung folgendermaßen aus:

q_{i+1}	r_i	x_i	y_i
	73685	1	0
2	25513	0	1
1	22659	1	-2
7	2854	-1	3
1	2681	8	-23
15	173	-9	26
2	86	143	-413
86	1	-295	852

Kapitel 2

Kongruenzen

2.1 Einleitung

Die Division mit Rest ergibt eine Partition der Menge $\mathbb{Z}$ der ganzen Zahlen in Äquivalenzklassen, Restklassen oder Kongruenzklassen genannt.

Definition 2.1.1. Es sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Wir sagen a ist kongruent zu b modulo m, wenn $m|(b-a)$ gilt, und wir schreiben $a \equiv b \mod m$ (bzw. $a \not\equiv b \mod m$, falls $m \not| (b-a)$ ist). Für die Menge aller b mit $a \equiv b \mod m$ schreiben wir $a \mod m$. In diesem Zusammenhang nennt man m den Modul der Kongruenz $a \equiv b \mod m$.

Satz 2.1.2. *Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ und die Divisionen*

$$\begin{aligned} a &= q_1 m + r_1 \text{ mit } 0 \leq r_1 < m \\ b &= q_2 m + r_2 \text{ mit } 0 \leq r_2 < m \end{aligned}$$

durch m mit Rest vorgelegt. Dann gilt $a \equiv b \mod m$ genau dann, wenn $r_1 = r_2$ ist.

Bemerkung 2.1.3. Zwei Zahlen $a, b \in \mathbb{Z}$ sind also genau dann kongruent modulo m, wenn sie bei der Division durch m den gleichen Rest haben.

Definition 2.1.4. Zwei Zahlen gehören zur selben Kongruenzklasse oder Restklasse modulo m, falls sie modulo m kongruent sind.

Satz 2.1.5. *Es sei $m \in \mathbb{N}$. Dann gibt es genau m Kongruenzklassen modulo m. Jede ganze Zahl ist zu genau einer der Zahlen $0, 1, \ldots, m-1$ kongruent.*

Beispiel 2.1.6. Die Kongruenzklassen modulo 2 sind

$$\begin{aligned} 0 \mod 2 &= \{\ldots, -4, -2, 0, 2, 4, \ldots\} \text{ (gerade Zahlen)} \\ 1 \mod 2 &= \{\ldots, -3, -1, 1, 3, 5, \ldots\} \text{ (ungerade Zahlen).} \end{aligned}$$

Die Kongruenzklassen modulo 10 sind

$$\begin{aligned} 0 \mod 10 &= \{\ldots, -20, -10, 0, 10, 20, \ldots\} \\ 1 \mod 10 &= \{\ldots, -19, -9, 1, 11, 21, \ldots\} \\ &\vdots \quad\quad \vdots \\ 9 \mod 10 &= \{\ldots, -11, -1, 9, 19, 29, \ldots\} \end{aligned}$$

Allgemein sind Kongruenzklassen modulo m arithmetische Progressionen der Form

$$a \mod m = \{\ldots, a-3m, a-2m, a-m, a, a+m, a+2m, \ldots\}$$

Definition 2.1.7. Es sei $m \in \mathbb{N}$. Die Menge aller Restklassen modulo m bezeichnen wir mit $\mathbb{Z}/m\mathbb{Z}$.

Es ist möglich, Restklassen zu addieren und zu multiplizieren:
Die Addition läßt sich einfach auf geometrische Weise veranschaulichen. Wickelt man die Zahlengerade über einem Kreis des Umfangs m auf, so bestehen Restklassen $\mod m$ genau aus den Zahlen, die über demselben Punkt des Kreises zu liegen kommen.
Die Summe $a \mod m + b \mod m$ erhält man, indem man auf dem Kreis nacheinander a Schritte und b Schritte in die negative Richtung geht.

Beispiel 2.1.8. Das Rechnen mit Uhrzeiten bedeutet Rechnen mit Restklassen $\mod 24$ oder bei der alten Weise, bei der die Stunden nur von $1-12$ numeriert werden, Rechnen mit Restklassen $\mod 12$. Welche Uhrzeit haben wir sieben Stunden nach 9 Uhr? Die Antwort erhalten wir, wenn wir den Stundenzeiger von 9 Uhr um sieben Stunden im Uhrzeigersinn (dem negativen Sinn) bewegen: 4 Uhr. Mittels Addition von Restklasen ergibt sich das Resultat wie folgt:

$$9 \mod 12 + 7 \mod 12 \equiv 4 \mod 12.$$

Beispiel 2.1.9. Das Rechnen mit Wochentagen bedeutet Rechnung mit Restklassen $\mod 7$:
Der 3. November 2009 ist ein Dienstag. Auf welchen Wochentag fällt der 25. November 2009?
Lösung:
Ordnen wir die Sonntage der Restklasse $0 \mod 7$ zu, so gehört der 3. November zur Restklasse $2 \mod 9$. Die Aufgaben läuft auf die Addition $2 \mod 7 + 22 \mod 7 = 2 \mod 7 + 1 \mod 7 = 3 \mod 7$ hinaus. Der 25. November 2009 fällt also auf einen Mittwoch.

Addition und Multiplikation von Restklassen können mit Hilfe von Verknüpfungstafeln tabelliert werden:

Beispiel 2.1.10. $m = 5$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

2.2 Das multiplikative Inverse

Definition 2.2.1. (multiplikatives Inverses)
Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Es heißt $b \mod m$ muliplikatives Inverses von $a \mod m$, falls $ab \equiv 1 \mod m$ ist.
Wir schreiben dann auch $b \mod m = a^{-1} \mod m$.

Beispiel 2.2.2. Die Multiplikationstafel in Beispiel 2.1.10 zeigt, daß das multiplikative Inverse von 2 mod 5 gerade $3 \mod 5$ ist. Also gilt $2^{-1} \mod 5 = 3 \mod 5$.

Das multiplikative Inverse braucht nicht immer zu existieren. Näheres ergibt sich aus dem folgenden

Satz 2.2.3. *Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Das multiplikative Inverse $a^{-1} \mod m$ existiert genau dann, wenn $ggT(a, m) = 1$ ist.*
Zur Berechnung des multiplikativen Inversen von $a \mod m$ löst man die Diophantische Gleichung $ax + by = 1$ nach dem in Satz 1.4.4 beschriebenen Verfahren. Dann ist $x \mod m = a^{-1} \mod m$.

Beispiel 2.2.4. Bestimme das multiplikative Inverse von $23 \mod 79$.
Lösung:
Wir müssen die Diophantische Gleichung

$$23x + 79y = 1 \qquad (*)$$

lösen.
Der Euklidische Algorithmus ergibt

$$\begin{aligned} 79 &= 3 \cdot 23 + 10 \\ 23 &= 2 \cdot 10 + 3 \\ 10 &= 3 \cdot 3 + 1 \end{aligned}$$

Auflösen der Gleichungen ergibt

$$1 = 10 - 3 \cdot 3 = 10 - 3 \cdot (23 - 2 \cdot 10) = 7 \cdot 10 - 3 \cdot 23 = 7 \cdot (79 - 3 \cdot 23) - 3 \cdot 23 = 7 \cdot 79 - 24 \cdot 23$$

Eine Lösung von $(*)$ ist also durch $x = -24$ und $y = 7$ gegeben.
Das multiplikative Inverse von $23 \mod 79$ ist also $23^{-1} \mod 79 = -24 \mod 79 = 55 \mod 79$.

2.3 Das Rechnen mit Kongruenzen

Kongruenzen machen eine Aussage über die Gleichheit von Restklassen und haben daher viel mit Gleichungen gemeinsam. Man kann mit ihnen weitgehend wie mit Gleichungen rechnen; es gibt jedoch auch Unterschiede. Dies wollen wir im folgenden diskutieren.

Satz 2.3.1. *Es seien $a, b, c, d, m \in \mathbb{Z}$, $m > 0$ mit $a \equiv b \mod m$ und $c \equiv d \mod m$. Dann ist*

$$\begin{aligned} a + c &\equiv b + d \mod m \\ a - c &\equiv b - d \mod m \\ a \cdot c &\equiv b \cdot d \mod m \end{aligned}$$

Gemeinsame Faktoren können in Kongruenzen nicht immer gekürzt werden.

Beispiel 2.3.2. Es ist $3 \cdot 5 \equiv 3 \cdot 2 \mod 9$, aber nicht $5 \equiv 2 \mod 9$.

Gemeinsame Faktoren können jedoch gekürzt werden, wenn man zu einem anderen Modul übergeht.

Satz 2.3.3. *Es seien $a, b, c, m \in \mathbb{Z}$, $m > 0$ und $d = ggT(c, m)$ und $ac \equiv bc \mod m$.*
Dann ist $a \equiv b \mod m/d$.
Spezialfall: Ist $ac \equiv bc \mod m$ und $ggT(c, m) = 1$, so ist $a \equiv b \mod m$.

Als Spezialfall von Satz 2.3.1 ergibt sich

Satz 2.3.4. *Es seien $a, b, m \in \mathbb{Z}$, $m > 0$.*
Aus $a \equiv b \mod m$ folgt $a^k \equiv b^k \mod m$ für $k \geq 1$.

Satz 2.3.4 erlaubt es, die Restklasse von a^k auch für große Werte von k zu bestimmen. Dazu wird k als Summe von Zweierpotenzen geschrieben. Die Restklassen von a^{2^δ} werden durch wiederholtes Quadrieren bestimmt.

Beispiel 2.3.5. Man bestimme $7^{52} \mod 53$.
Lösung:
Es ist $52 = 32 + 16 + 4$. Man berechnte 7^{32}, 7^{16} und 7^4 durch wiederholtes Quadrieren:

$$\begin{aligned} 7^2 &\equiv 49 \equiv -4 \mod 53 \\ 7^4 &\equiv (-4)^2 \equiv 16 \mod 53 \\ 7^8 &\equiv 16^2 \equiv -9 \mod 53 \\ 7^{16} &\equiv (-9)^2 \equiv -25 \mod 53 \\ 7^{32} &\equiv (-25)^2 \equiv -11 \mod 53, \end{aligned}$$

also

$$7^{52} \equiv 7^{32} \cdot 7^{16} \cdot 7^4 \equiv (-11) \cdot (-25) \cdot 16 \equiv 275 \cdot 16 \equiv 10 \cdot 16 \equiv 1 \mod 53.$$

2.4 Elementare Teilbarkeitsregeln

Die elementaren Teilbarkeitsregeln lassen sich durch Rechnen mit Kongruenzen leicht beweisen. Wir legen unseren Überlegungen die Darstellung natürlicher Zahlen im Dezimalsystem zugrunde.

Satz 2.4.1. *Jede natürliche Zahl $n \in \mathbb{N}$ kann eindeutig geschrieben werden als $n = \sum_{k=0}^{m} a_k 10^k$ mit $a_k \in \{0, 1, \ldots, 9\}$ und $a_m \neq 0$.*
Die a_k heißen die Ziffern von n (im Dezimalsystem).

Beispiel 2.4.2.

$$n = 283967 = 2 \cdot 10^5 + 8 \cdot 10^4 + 3 \cdot 10^3 + 9 \cdot 10^2 + 6 \cdot 10 + 7.$$

Definition 2.4.3. Unter der Quersumme einer Zahl $n = \sum_{k=0}^{m} a_k 10^k$ mit Ziffern a_k versteht man $Q(n) = \sum_{k=0}^{m} a_k$.

Unter der alternierenden Quersumme versteht man $AQ(n) = \sum_{k=0}^{m} (-1)^k a_k$.

Satz 2.4.4. (a) *Eine natürliche Zahl n ist genau dann durch 2 teilbar (gerade), wenn die letzte Ziffer durch 2 teilbar (gerade) ist.*

(b) *Eine Zahl n ist genau dann durch 5 teilbar, wenn die letzte Ziffer 0 oder 5 ist.*

(c) *Eine Zahl n ist genau dann durch 3 teilbar, wenn ihre Quersumme durch 3 teilbar ist.*

(d) *Eine Zahl n ist genau dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.*

(e) *Eine Zahl n ist genau dann durch 11 teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.*

Beweis. Wir nehmen $n = \sum_{k=0}^{m} a_k 10^k$, $a_k \in \{0, 1, \ldots, m-1\}$ und $a_m \neq 0$ an.

(a) Wegen $10^k \equiv \begin{cases} 0 \mod 2, & \text{für } k \geq 1 \\ 1 \mod 2, & \text{für } k = 0 \end{cases}$ folgt $n \equiv a_0 \mod 2$.

(b) Wegen $10^k \equiv \begin{cases} 0 \mod 5, & \text{für } k \geq 1 \\ 1 \mod 5, & \text{für } k = 0 \end{cases}$ folgt $n \equiv a_0 \mod 5$.

(c) Es ist $10 \equiv 1 \mod 3$. nach Satz 2.3.4 folgt $10^k \equiv 1 \mod 3$. Damit ist $n = \sum_{k=0}^{m} a_k 10^k = \sum_{k=0}^{m} a_k \mod 3$ nach Satz 2.3.1.

(d) Es ist $10 \equiv 1 \mod 9$. Die Behauptung folgt wie in c), wenn Kongruenzen $\mod 3$ durch Kongruenzen $\mod 9$ ersetzt werden.

(e) Es ist $10 \equiv -1 \mod 11$. Nach Satz 2.3.4 folgt $10^k \equiv (-1)^k \mod 11$. Damit ist $n = \sum_{k=0}^{m} a_k 10^k = \sum_{k=0}^{m} (-1)^k a_k \mod 11$.

□

2.5 Restsysteme, teilerfremde Restklassen, Eulersche φ- Funktion

Wir haben in Satz 2.1.5 gesehen, daß es genau m Kongruenzklassen modulo m gibt und daß jede ganze Zahl zu genau einer der Zahlen $0, 1, \ldots, m-1$ kongruent ist. Jede Restklasse $\mod m$ wird also durch genau ein Element der Menge $R_m = \{0, 1, \ldots, m-1\}$ repräsentiert. Die Menge R_m ist ein (wichtiger) Spezialfall eines vollständigen Restsystems modulo m.

Definition 2.5.1. Ein vollständiges Restsystem $\mod m$ ist eine Menge ganzer Zahlen, so daß jede ganze Zahl zu genau einer dieser Zahlen der Menge kongruent $\mod m$ ist.

Beispiel 2.5.2. Das vollständige Restsystem $\{0, 1, \ldots, m-1\}$ heißt auch die Menge der kleinsten nichtnegativen Reste $\mod m$.
Es sei m eine ungerade positive Zahl. Dann ist die Menge der absolut kleinsten Reste $\{-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2}\}$ ein vollständiges Restsystem $\mod m$.
Für $m = 5$ ist also die Menge der kleinsten nichtnegativen Reste $\mod 5$ die Menge $\{0, 1, 2, 3, 4\}$, und die Menge der absolut kleinsten Reste $\mod 5$ ist die Menge $\{-2, -1, 0, 1, 2\}$.
Ein weiteres vollständiges Restsystem $\mod 5$ ist die Menge $\{100, -24, 12, 33, -71\}$.

Eine wichtige Frage ist nun: Welchen größten gemeinsamen Teiler beitzen die Elemente eines vollständigen Restsystems $\mod m$ mit dem Modul m?

Beispiel 2.5.3. $m = 12$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$ggT(a, 12)$	12	1	2	3	4	1	6	1	4	3	2	1

Der $ggT(a, 12)$ hängt nur von der Restklasse $a \mod 12$ ab:
Für alle Elemente von $0 \mod 12 = \{\ldots, -12, 0, 12, 24, 36, \ldots\}$ ist $ggT(a, 12) = 12$.
Für alle Elemente von $3 \mod 12 = \{\ldots, -9, 3, 15, 27, \ldots\}$ ist $ggT(a, 12) = 3$.
Es ist $ggT(a, 12) = 1$ für die Elemente der vier teilerfremden Restklassen $1 \mod 12$, $5 \mod 12$, $7 \mod 12$ und $11 \mod 12$.

Diese Tatsachen ergeben sich als Spezialfall aus

Satz 2.5.4. *Es sei $m \in \mathbb{N}$. Ist $a \equiv b \mod m$, so ist $ggT(a, m) = ggT(b, m)$, d.h. $ggT(a, m) = ggT(b, m)$ für alle $b \in a \mod m$.*

Definition 2.5.5. Es sei $m \in \mathbb{N}$. Gilt $ggT(b, m) = 1$ für ein Element- und damit für alle Elemente- $b \in a \mod m$, so heißt $a \mod m$ eine teilerfremde Restklasse $\mod m$. Die Anzahl der teilerfremden Restklassen wird mit $\varphi(m)$ bezeichnet. Dabei heißt $\varphi(m)$ Eulersche φ- Funktion.
Ein reduziertes Restsystem $\mod m$ ist eine Menge ganzer Zahlen, so daß jede zu m teilerfremde ganze Zahl zu genau einer dieser Zahlen der Menge kongruent ist.

Beispiel 2.5.6. Beispiel 2.5.3 zeigt, daß $\varphi(12) = 4$ ist. Ein reduziertes Restsystem ist durch $\{1, 5, 7, 11\}$ gegeben. Ein anderes reduziertes Restsystem ist $\{-23, 17, 31, 47\}$.

2.6 Lineare Kongruenzen

Es seien $a, b, m \in \mathbb{Z}$ mit $m > 0$. Wir suchen alle ganzen Zahlen x, welche die lineare Kongruenz

$$ax \equiv b \mod m \qquad (*)$$

erfülllen.
Ob x eine Lösung von $(*)$ ist, hängt nur von der Restklasse $\mod m$ von x ab: $(*)$ wird entweder von allen Elementen einer Restklasse $\mod m$ gelöst oder von keinem. Alles läuft daher auf die Frage hinaus: Welche Restklassen sind Lösungen? Man spricht auch von Lösungen $\mod m$.

Satz 2.6.1. *Es seien $a, b, m \in \mathbb{Z}$ mit $m > 0$ und $d = ggT(a, m)$. Die Kongruenz $ax \equiv b \mod m$ ist genau dann lösbar, wenn $d|b$. Ist diese Bedingung erfüllt, so bilden die Lösungen eine arithmetische Progression mit Differenz m/d. Es gibt also d Lösungen $\mod m$.*

Bemerkung 2.6.2. Im Falle der Lösbarkeit können die Lösungen mittels Satz 2.3.3 erhalten werden:
Die Kongruenz $ax \equiv b \mod m$ ist äquivalent zu $a/d\ x \equiv b/d \mod m/d$.
Die Kongruenz kann gelöst werden, in dem man mit der Methode von Abschnitt 2.2 das multiplikative Inverse von $a/d \mod m/d$ bestimmt- bei kleinen Werten von m/d auch durch Probieren.

Beispiel 2.6.3.

$$15x \equiv 6 \mod 21 \qquad (1)$$

Es ist $a = 15$, $b = 6$ und $m = 21$. Also ist $d = ggT(15, 21) = 3$, somit $d|6$.
Nach Satz 2.3.3 (oder Bemerkung 2.6.2) ist (1) äquivalent zu

$$5x \equiv 2 \mod 7. \tag{2}$$

Das multiplikative Inverse von 5 mod 7 ergibt sich als

$$5^{-1} \mod 7 = 3 \mod 7,$$

da $5 \cdot 3 \equiv 1 \mod 7$.
Damit ist $x \equiv 2 \cdot 5^{-1} \mod 7 \equiv 2 \cdot 3 \mod 7 \equiv 6 \mod 7$ die eindeutige Lösung von (2). Die Lösungen der ursprünglichen Kongruenz (1) sind die drei Restklassen 6 mod 21, 13 mod 21 und 20 mod 21. Deren Elemente ergeben zusammen die arithmetische Progression $\{\ldots, -15, -8, -1, 6, 13, 20, \ldots\}$ mit der Differenz $m/d = 7$.

2.7 Der Chinesische Restsatz

Der Chinesische Restsatz befaßt sich mit Systemen von Kongruenzen.

Beispiel 2.7.1. Es sei $N = 35 = 5 \cdot 7$.
Erfüllt eine ganze Zahl m eine Kongruenz mod 35, so erfüllt m auch ein Paar von Kongruenzen, eine Kongruenz mod 5 und eine Kongruenz mod 7.
Ist z. B.

$$m \equiv 13 \mod 35, \tag{1}$$

so folgt

$$\begin{cases} m \equiv 3 \mod 5 \\ m \equiv 6 \mod 7. \end{cases} \tag{2}$$

Die folgende Tabelle zeigt, daß auch (1) aus (2) folgt. Schärfer gilt, daß jedem Paar von Restklassen (a mod 5, b mod 7) genau eine Restklasse c mod 35 entspricht.

Tabelle 2.7.2.

mod 5 \ mod 7	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

Jede Restklasse mod 35 hat somit zwei Komponenten, eine (mod 7)- Komponente und eine (mod 5)-Komponente. Eine ähnliche Situation besteht in der Vektorrechnung: jeder Punkt der Ebene kann mit einem Koordinatenpaar (x, y) oder auch dem Vektor $\vec{v} = (x, y)$ identifiziert werden. Mit Vektoren kann komponentenweise gerechnet werden: Für $\vec{v}_1 = (x_1, y_1)$ und $\vec{v}_2 = (x_2, y_2)$ ist $\vec{v}_1 + \vec{v}_2 = (x_1 + x_2, y_1 + y_2)$. Dieses „komponentenweise“ Rechnen ist auch bei Kongruenzen möglich:

Beispiel 2.7.3. Man bestimme das Produkt

$$(23 \mod 35) \cdot (29 \mod 35).$$

Lösung:
Aus der Tabelle 2.7.2 erhalten wir die Entsprechungen

$$\begin{aligned} 23 \mod 35 &\Leftrightarrow (2 \mod 7, \quad 3 \mod 5) \\ 29 \mod 35 &\Leftrightarrow (1 \mod 7, \quad 4 \mod 5) \end{aligned}$$

Komponentenweises Rechnen ergibt

$$(2 \mod 7, \quad 3 \mod 5) \cdot (1 \mod 7, \quad 4 \mod 5) = (2 \mod 7, \quad 2 \mod 5).$$

Mit der Entsprechung

$$2 \mod 35 \Leftrightarrow (2 \mod 7, \quad 2 \mod 5).$$

erhalten wir

$$(23 \mod 35) \cdot (29 \mod 35) = 2 \mod 35.$$

Wir formulieren nun den Chinesischen Restsatz allgemein und geben auch einen Algorithmus, der ein System von Kongruenzen zu einer einzelnen Kongruenz reduziert.

Satz 2.7.4. *(Chinesischer Restsatz) Es seien $m_1, m_2, \ldots, m_r$ natürliche Zahlen, die paarweise teilerfremd sind und $a_1, a_2, \ldots, a_r$ ganze Zahlen. Dann besitzen die r Kongruenzen*

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \\ &\vdots \quad\quad \vdots \\ x &\equiv a_{r-1} \mod m_{r-1} \\ x &\equiv a_r \mod m_r \end{aligned}$$

eine gemeinsame Lösung.
Diese ist nach dem Modul

$$m = m_1 \cdot m_2 \cdots m_r$$

eindeutig bestimmt.
Eine Lösung kann in der Form

$$x_0 = \sum_{j=1}^{r} M_j M_j^{-1} a_j$$

erhalten werden, wobei

$$M_j := \frac{m}{m_j}, \quad \textit{und} \quad M_j M_j^{-1} \equiv 1 \mod m_j$$

ist.

Beispiel 2.7.5. Gesucht ist die kleinste natürliche Zahl x mit

$$\begin{aligned} x &\equiv 4 \mod 7 \\ x &\equiv 1 \mod 11 \\ x &\equiv 6 \mod 13 \end{aligned}$$

Lösung:
Mit den Bezeichnungen von Satz 2.7.4 ist $m_1 = 7$, $m_2 = 11$, $m_3 = 13$, $m = 7 \cdot 11 \cdot 13 = 1001$, $a_1 = 4$, $a_2 = 1$ und $a_3 = 6$. Weiter ist

$$\begin{aligned} M_1 &:= \frac{m}{m_1} = 143 \\ M_2 &:= \frac{m}{m_2} = 91 \\ M_3 &:= \frac{m}{m_3} = 77. \end{aligned}$$

Die Bestimmung der multiplikativen Inversen M_j^{-1} ist wiederum mit der Methode von Abschnitt 2.2, also dem Euklidischen Algorithmus möglich. Da in unserem speziellen Beispiel die Moduln $m_1 = 7$, $m_2 = 11$ und $m_3 = 13$ klein sind, können hier die Lösungen auch durch Probieren gefunden werden:

$$\begin{aligned} 143 \cdot M_1^{-1} \equiv 1 \mod 7 &\Leftrightarrow 3 \cdot M_1^{-1} \equiv 1 \mod 7, \text{ also } M_1^{-1} \equiv -2 \mod 7 \\ 91 \cdot M_2^{-1} \equiv 1 \mod 11 &\Leftrightarrow 3 \cdot M_2^{-1} \equiv 1 \mod 11, \text{ also } M_2^{-1} \equiv 4 \mod 11 \\ 77 \cdot M_3^{-1} \equiv 1 \mod 13 &\Leftrightarrow -M_3^{-1} \equiv 1 \mod 13, \text{ also } M_3^{-1} \equiv -1 \mod 13. \end{aligned}$$

Wir erhalten die Lösung

$$x_0 = \sum_{j=1}^{3} M_j M_j^{-1} a_j = 143 \cdot (-2) \cdot 4 + 91 \cdot 4 \cdot 1 + 77 \cdot (-1) \cdot 6 = -1242.$$

Die allgemeine Lösung hat die Form

$$x = x_0 + k \cdot m = -1242 + 1001k.$$

Die kleinste positive Lösung erhalten wir für $k = 2$, nämlich $x = 760$.

2.8 Berechnung der Eulerschen φ- Funktion, Multiplikativität

Auch die Frage, welche Restklassen eines vollständigen Restsystems reduziert sind, kann mit der Idee des „komponentenweisen Rechnens“, also des Chinesischen Restsatzes beantwortet werden.
Wir kehren zu unserem alten Beispiel $N = 35 = 5 \cdot 7$ zurück. Es ist genau dann $ggT(a, 35) = 1$, wenn $ggT(a, 7) = 1$ und $ggT(a, 5) = 1$ ist. Es gilt $ggT(a, 5) = 1$, wenn die Restklasse $a \mod 5$ nicht in der ersten Zeile der Tabelle 2.7.2 zu finden ist, und es gilt $ggT(a, 7) = 1$, wenn die Restklasse $a \mod 7$ nicht in der ersten Spalte der Tabelle 2.7.2 zu finden ist.
Für die Wahl der Zeilen haben wir also $\varphi(5) = 4$ Möglichkeiten und für die Wahl des Spalten $\varphi(7) = 6$ Möglichkeiten.
Es ist somit

$$\varphi(35) = \varphi(5 \cdot 7) = \varphi(5) \cdot \varphi(7) = 24.$$

Diese Multiplikativität gilt für die Eulersche φ- Funktion allgemein.

Definition 2.8.1. Eine Abbildung $f : \mathbb{N} \to \mathbb{C}$ heißt zahlentheoretische (oder arithmetische) Funktion. Diese Funktion f heißt additiv, falls

$$f(m \cdot n) = f(m) + f(n) \tag{1}$$

für alle $m, n \in \mathbb{N}$ mit $ggT(m, n) = 1$ gilt.
Sie heißt vollständig additiv, falls (1) ohne Einschränkung gilt.

Die Funktion f heißt multiplikativ, falls

$$f(m \cdot n) = f(m) \cdot f(n) \tag{2}$$

für alle $m, n \in \mathbb{N}$ mit $ggT(m, n) = 1$ gilt.
Sie heißt vollständig multiplikativ, falls (2) ohne Einschränkung gilt.

Satz 2.8.2. *Es sei $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ die kanonische Primfaktorzerlegung von n. Ist f additiv, so ist $f(1) = 0$ und $f(n) = f(p_1^{\gamma_1}) + \ldots + f(p_r^{\gamma_r})$. Ist f multiplikativ, so ist $f(1) = 1$ und $f(n) = f\left(p_1^{\gamma_1}\right) \cdots f\left(p_r^{\gamma_r}\right)$.*
Dies läßt sich nun auf die Eulersche φ- Funktion anwenden. Wir betrachten zunächst ihre Werte für Primzahlpotenzen p^γ. Von der Menge der kleinsten nichtnegativen Reste $\{0, 1, \ldots, p^\gamma - 1\}$ sind genau die $p^{\gamma-1}$ Vielfachen von p nicht teilerfremd zum Modul p^γ. Also ist

$$\varphi\left(p^\gamma\right) = p^\gamma - p^{\gamma-1} = p^\gamma \cdot \left(1 - \frac{1}{p}\right). \tag{1}$$

Ist $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$, so folgt aus der Multiplikativität von φ:

$$\varphi(n) = p_1^{\gamma_1} \cdot \left(1 - \frac{1}{p_1}\right) \cdots p_r^{\gamma_r} \cdot \left(1 - \frac{1}{p_r}\right) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Satz 2.8.3. *Die Eulersche φ- Funktion ist multiplikativ. Es ist $\varphi(1) = 1$. Ist $n = p_1^{\gamma_1} \cdots p_r^{\gamma_r}$ die kanonische Primfaktorzerlegung von n, so ist*

$$\varphi(n) = \left(p_1^{\gamma_1} - p_1^{\gamma_1 - 1}\right) \cdots \left(p_r^{\gamma_r} - p_r^{\gamma_r - 1}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Beispiel 2.8.4. Man bestimme $\varphi(9000)$.

Lösung:
Es ist $9000 = 2^3 \cdot 3^2 \cdot 5^3$.
Also ist $\varphi(9000) = \left(2^3 - 2^2\right) \cdot \left(3^2 - 3\right) \cdot \left(5^3 - 5^2\right) = 2400$.

2.9 Die Sätze von Euler und Fermat

Der kleine Satz von Fermat (Pierre de Fermat, ca. 1607-1665) wurde etwa 100 Jahre vor dem Satz von Euler (Leonhard Euler, 1707-1783) gefunden und ist einfacher zu formulieren. Jedoch ist der kleine Satz von Fermat ein Spezialfall des Satzes von Euler.

Satz 2.9.1. *(Satz von Euler)*
Es sei $m \in \mathbb{N}$, $a \in \mathbb{Z}$ und $ggT(a, m) = 1$. Dann ist

$$a^{\varphi(m)} \equiv 1 \mod m.$$

Spezialfall (kleiner Fermat):
Es sei p eine Primzahl und $a \in \mathbb{Z}$ nicht durch p teilbar. Dann ist

$$a^{p-1} \equiv 1 \mod p.$$

Der Beweis des Satzes von Euler bietet eine gute Gelegenheit zur Anwendung der Konzepte der letzten Abschnitte.

Lemma 2.9.2. *Es sei $m \in \mathbb{N}$, $R_1 = \{r_1, \ldots, r_{\varphi(m)}\}$ ein reduziertes Restsystem $\mod m$ und $ggT(a, m) = 1$. Dann ist auch $R_2 = \{ar_1, \ldots, ar_{\varphi(m)}\}$ ein reduziertes Restsystem $\mod m$.*

Bemerkung 2.9.3. Eine entsprechende Behauptung gilt auch für vollständige Restsystem $\mod m$.

Beweis. (Beweis von Lemma 2.9.2:)
Wegen $ggT(a, m) = 1$ folgt nach Satz 2.3.3:

$$ar_i \equiv ar_j \mod m \Leftrightarrow r_i \equiv r_j \mod m.$$

Damit sind die teilerfremden Restklassen $(ar_1) \mod m, \ldots, (ar_{\varphi(m)}) \mod m$ alle voneinander verschieden. Da die Gesamtzahl aller teilerfremden Restklassen $\varphi(m)$ ist, ist durch R_2 jede von ihnen genau einmal vertreten. □

Beweis. (Beweis von Satz 2.9.1:)
Es sei $R_1 = \{r_1, \ldots, r_{\varphi(m)}\}$ ein reduziertes Restsystem. Dann ist nach Lemma 2.9.2 auch $R_2 = \{ar_1, \ldots, ar_{\varphi(m)}\}$ ein reduziertes Restsystem.
Somit folgt

$$\begin{aligned} ar_1 &\equiv r_{i_1} \mod m \\ ar_2 &\equiv r_{i_2} \mod m \\ \vdots &\quad \vdots \\ ar_{\varphi(m)} &\equiv r_{i_{\varphi(m)}} \mod m \end{aligned}$$

wobei die Folge $(i_1, i_2, \ldots, i_{\varphi(m)})$ eine Umordnung der Folge $(1, 2, \ldots, \varphi(m))$ ist. Multiplikation der obigen Kongruenzen ergibt somit

$$a^{\varphi(m)}(r_1 \cdots r_{\varphi(m)}) \equiv (r_1 \cdots r_{\varphi(m)}) \mod m.$$

Da das Produkt $(r_1 \cdots r_{\varphi(m)})$ teilerfremd zu m ist, kann es gekürzt werden. Wir erhalten

$$a^{\varphi(m)} \equiv 1 \mod m.$$

□

Kapitel 3

Algebraische Grundstrukturen in der Zahlentheorie

3.1 Algebraische Grundstrukturen

Definition 3.1.1. Es sei $X \neq \emptyset$. Auf X sei eine (innere) Verknüpfung $\circ$, d.h. eine Abbildung $\circ : X \times X \to X,\ (x, y) \to x \circ y$ definiert.

1. $(X, \circ)$ heißt Halbgruppe, falls die Verknüpfung $\circ$ dem Assoziativgesetz genügt:
$$\forall x, y, z \in X :\ (x \circ y) \circ z = x \circ (y \circ z).$$
2. Ein $e \in X$ heißt neutrales Element der Halbgruppe, falls $e \circ x = x \circ e = x$ für alle $x \in X$ gilt.
3. Ein $x \in X$ heißt Einheit, falls es ein Inverses $x^{-1} \in X$ mit $x \circ x^{-1} = x^{-1} \circ x = e$ gibt.
4. $(X, \circ)$ heißt abelsche oder kommutative Halbgruppe, falls $x \circ y = y \circ x$ für alle $x, y \in X$ gilt.
5. Jede Halbgruppe mit neutralem Element, die nur Einheiten besitzt, heißt Gruppe.

Beispiel 3.1.2. $(\mathbb{N}, +)$ besitzt die einzige Einheit 0, ist also keine Gruppe, sondern nur eine kommutative Halbgruppe.
$(\mathbb{Z}, +)$ ist hingegen eine kommutative Gruppe- mit neutralem Element 0 und den Negativen $-a$ als Inverse zu $a \in \mathbb{Z}$.
$(\mathbb{N}, \cdot)$ und $(\mathbb{Z}, \cdot)$ sind kommutative Halbgruppen mit neutralem Element 1, aber keine Gruppen.

Bemerkung 3.1.3. Es ist üblich, die Verknüpfung nur dann mit $+$ zu bezichnen, also als Addition zu betrachten, wenn sie kommutativ ist. Existiert ein neutrales Element, so nennt man es 0. Zur Bezeichnung der Inversen verwendet man das Minuszeichen.

Wir kommen nun zu Strukturen mit zwei inneren Verknüpfungen.

Definition 3.1.4. Es sei $X \neq \emptyset$ eine Menge mit zwei inneren Verknüpfungen, der Addition $+$ und der Multiplikation $\cdot$. Dann definiert man

1. $(X, +, \cdot)$ heißt ein Ring, falls gilt:
   (a) $(X, +)$ ist eine abelsche Gruppe

(b) $(X, \cdot)$ ist eine Halbgruppe

(c) es gelten die Distributivgesetze $(a+b)\cdot c = (a\cdot c)+(a\cdot b)$ und $c\cdot(a+b) = (c\cdot a)+(c\cdot b)$ für alle $a, b, c \in X$.

5. Das neutrale Element von $(X, +)$ heißt Null (Schreibweise: 0).

6. Besitzt $(X, \cdot)$ ein neutrales Element, so heißt dieses Eins (Schreibweise: 1).

7. Ist $(X, \cdot)$ abelsch, so heißt $(X, +, \cdot)$ ein kommutativer Ring.

8. Der Ring $(X, +, \cdot)$ heißt nullteilerfrei, falls für alle $x, y \in X$ gilt

$$x \cdot y = 0 \Rightarrow x = 0 \text{ oder } y = 0.$$

9. Ein nullteilerfreier und kommutativer Ring, der mindestens zwei verschiedene Elemente enthält, heißt Integritätsring.

10. Ein Integritätsring mit 1, in dem jedes $a \neq 0$ eine (multiplikative) Einheit ist, heißt Körper.

Beispiel 3.1.5. $(\mathbb{N}, +, \cdot)$ ist kein Ring, da $(\mathbb{N}, +)$ keine Gruppe ist.
$(\mathbb{Z}, +\cdot)$ ist ein Integritätsring mit 1, aber kein Körper. Die einzigen multiplikativen Einheiten sind 1 und -1.
$(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ bzw. $(\mathbb{C}, +, \cdot)$ sind die Körper der rationalen, reellen bzw. komplexen Zahlen.

3.2 Beispiele in der Zahlentheorie

Es sei $m \in \mathbb{N}$.
Es ist klar, daß die Restklassenmenge $\mathbb{Z}/m\mathbb{Z}$ eine abelsche Gruppe bzgl. der Addition bildet. Das neutrale Element ist die Restklasse $0 \mod m$. Es bildet $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ einen kommutativen Ring, der die Restklasse $1 \mod m$ als Einselement hat. Ist m keine Primzahl, so ist der Ring nicht nullteilerfrei. Ist $m = k \cdot l$ mit $1 < k < m$ und $1 < l < m$, so haben wir

$$(k \mod m) \cdot (l \mod m) = m \mod m = 0 \mod m.$$

Nach Satz 2.2.3 existiert das multiplikative Inverse genau dann, wenn $a \mod m$ eine reduzierte Restklasse $\mod m$ ist, d.h. wenn $ggT(a, m) = 1$ ist.
Die Einheiten des Rings $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ sind also genau die reduzierten Restklassen $\mod m$. Ihre Menge bildet eine Gruppe bzgl. der Multiplikation.

Definition 3.2.1. Für $m \in \mathbb{N}$ bezeichnen wir mit $(\mathbb{Z}/m\mathbb{Z})^*$ die Menge der Einheiten des Rings $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$, also

$$(\mathbb{Z}/m\mathbb{Z})^* = \{a \mod m : \ ggT(a, m) = 1\}.$$

Offenbar hat $(\mathbb{Z}/m\mathbb{Z})^*$ genau $\varphi(m)$ Elemente.
Ist p eine Primzahl, so besteht $(\mathbb{Z}/m\mathbb{Z})^*$ aus allen Restklassen außer der 0- Restklasse $0 \mod p$. Damit ist aber $((\mathbb{Z}/p\mathbb{Z}), +, \cdot)$ ein endlicher Körper mit p Elementen.

Wir fassen unsere Beobachtungen zusammen:

Satz 3.2.2. *Es sei $m \in \mathbb{N}$. Dann ist $(\mathbb{Z}/m\mathbb{Z}, +)$ eine abelsche Gruppe mit m Elementen und neutralem Element $0 \mod m$. Es ist weiterhin $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring mit Einselement $1 \mod m$. Die Menge $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ bildet eine abelsche Gruppe mit $\varphi(m)$ Elementen. Der Ring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist genau dann ein Integritätsring und sogar ein Körper, wenn m eine Primzahl ist.*

3.3 Untergruppen, zyklische Gruppen, Ordnung und Primitivwurzel

Definition 3.3.1. Es sei $(G, \circ)$ eine Gruppe. Unter einer Untergruppe U von G versteht man eine Teilmenge $U \subseteq G$, die bzgl. der Verknüpfung $\circ$ ebenfalls eine Gruppe ist, d.h. $(U, \circ)$ ist eine Gruppe.
Schreibweise: $(U, \circ) \lhd (G, \circ)$.

Beispiel 3.3.2. Untergruppen der Gruppe $(\mathbb{Z}, +)$ sind alle Mengen der Gestalt

$$m\mathbb{Z} := \{m \cdot k : \ k \in \mathbb{Z}\},$$

wobei $m \in \mathbb{Z}$ fest gewählt ist.
Es ist

$$(\mathbb{Z}, +) \lhd (\mathbb{Q}, +) \lhd (\mathbb{R}, +).$$

Definition 3.3.3. Es sei $(G, \circ)$ eine Gruppe und $\mathcal{M} \subseteq G$ eine Teilmenge von G. Unter $\langle \mathcal{M} \rangle$, der von $\mathcal{M}$ erzeugten Untergruppe von G (Schreibweise: $\langle \mathcal{M} \rangle$), versteht man die kleinste Untergruppe von G, die $\mathcal{M}$ enthält. Ist $\mathcal{M}$ eine einelementige Menge $\mathcal{M} = \{g\}$ mit $g \in G$, so schreibt man auch anstelle von $\langle \{g\} \rangle$ einfach $\langle g \rangle$.

Beispiel 3.3.4. Es sei $\mathcal{M} = \{9, 15\}$. Dann ist die von $\mathcal{M}$ erzeugte Untergruppe $\langle \mathcal{M} \rangle$ von $(\mathbb{Z}, +)$ gegeben durch

$$\langle \mathcal{M} \rangle = 3\mathbb{Z} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}.$$

Dies sieht man wie folgt:
$\langle \mathcal{M} \rangle$ muß wegen seiner Untergruppeneigenschaft mit 9 und 15 auch die Vielfachen $27 = 9 + 9 + 9$ und $30 = 15 + 15$, und mit 27 und 30 auch die Differenz $3 = 30 - 27$ enthalten.

Definition 3.3.5. Eine Gruppe heißt zyklisch, wenn G von einem einzigen Element erzeugt wird, d.h. wenn gilt, daß $G = \langle g \rangle$ für ein $g \in G$. Dann heißt g auch erzeugendes Element oder auch Erzeugendes von G, und man sagt: G wird von g erzeugt.

Zur Formulierung des nächsten Satzes benötigen wir den Begriff der Potenz eines Elementes.

Definition 3.3.6. Es sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Es sei $g \in G$. Für $m \in \mathbb{Z}$, $m \geq 0$ definieren wir die Potenz g^m durch die Rekursion $g^0 = e$ und $g^{m+1} = (g^m) \cdot g$.
Für $m < 0$ setzen wir: $g^m = (g^{-m})^{-1}$.

Satz 3.3.7. *Es sei $(G, \circ)$ zyklisch mit neutralem Element e, also $G = \langle g \rangle$ für ein $g \in G$. Dann besteht g aus allen Potenzen von g:*

$$G = \{\ldots, g^{-2}, g^{-1}, g^0 = e, g, g^2, \ldots\}.$$

Es gibt nun zwei Hauptfälle:
Fall 1: Alle Potenzen g^k sind verschieden.
Fall 2: Es gibt $k_1 \neq k_2$, so daß $g^{k_1} = g^{k_2}$.

In beiden Fällen gibt es ein „Standardmodell“, von dem sich die gegebene Gruppe G höchstens durch die Namen ihrer Elemente und der Verknüpfung unterscheidet. Die Namensänderung wird durch einen Isomorphismus vermittelt. Dieser Begiff ist auch für andere algebraische Grundstrukturen grundlegend. Wir geben die Definition jedoch nur für Gruppen.

Definition 3.3.8. Es seien $(G, \circ)$ und $(G', *)$ Gruppen. Eine Abbildung $\Phi: (G, \circ) \to (G', *)$ heißt Isomorphismus, wenn Φ bijektiv und relationstreu ist, d.h. wenn gilt

$$\Phi(a \circ b) = \Phi(a) * \Phi(b)$$

für alle $a, b \in G$.
Es heißen $(G, \circ)$ und $(G', *)$ isomorph, wenn ein Isomorphismus $\Phi: G \to G'$ existiert.

Wir kommen nun zur Diskussion der zyklischen Gruppen $(G, \circ)$ mit $G = \langle g \rangle$.

Fall 1:
Alle Potenzen g^k sind verschieden.
Dann ist $(G, \circ)$ isomorph zum „Standardmodell" $(\mathbb{Z}, +)$. Der Isomorphismus Φ ist gegeben durch $\Phi: \mathbb{Z} \to G$, $n \to g^n$. Insbesondere ist $(\mathbb{Z}, +)$ selbst eine zyklsiche Gruppe mit den Erzeugenden 1 oder -1, d.h. $\mathbb{Z} = \langle 1 \rangle$ oder $\mathbb{Z} = \langle -1 \rangle$.

Fall 2:
Wir beginnen mit einem Beispiel:

Beispiel 3.3.9. Die Gruppe $G = ((\mathbb{Z}/7\mathbb{Z})^*, \cdot)$ wird von der Restklasse 3 mod 7 erzeugt, wie folgende Tabelle zeigt:

Tabelle 3.3.10.

k	0	1	2	3	4	5	6	7	
$3^k \mod 7$	1	3	2	6	4	5	1	3	mod 7.

Aus der Tabelle wird auch die Periodizität der Folge der Potenzen ersichtlich, die bei endlichen zyklischen Gruppen immer auftritt. $(\mathbb{Z}/7\mathbb{Z}, \cdot)$ ist isomorph zur Gruppe $(\mathbb{Z}/6\mathbb{Z}, +)$. Der Isomorphismus Φ ist gegeben durch:

$$\Phi: \ k \mod 6 \to 3^k \mod 7.$$

Hier haben wir also eine zyklische Gruppe G der Ordnung 6, die zu $(\mathbb{Z}/6\mathbb{Z}, +)$ isomorph ist. Allgemein ist eine zyklische Gruppe G der Ordnung m zu $(\mathbb{Z}/m\mathbb{Z}, +)$ isomorph.
Ist $G = \langle g \rangle$, so ist $G = \{e, g, \ldots, g^{m-1}\}$ und $\Phi: \mathbb{Z}/m\mathbb{Z} \to G, \ k \mod m \to g^k$ ein Isomorphismus.

Wir fassen unsere Ergebnisse zusammen in

Satz 3.3.11. *Eine unendliche zyklische Gruppe ist stets isomorph zur Gruppe $(\mathbb{Z}, +)$. Die Gruppe $(\mathbb{Z}, +)$ wird erzeugt von den Elementen 1 und -1: $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$. Die Potenzen von 1 bzw. -1 sind alle verschieden.*
Eine endliche zyklische Gruppe ist isomorph zu einer Gruppe $(\mathbb{Z}/m\mathbb{Z}, +)$ für ein festes $m \in \mathbb{N}$.
Es ist $\mathbb{Z}/m\mathbb{Z} = \langle 1 \mod m \rangle$.
Unter den Potenzen von $1 \mod m$ sind m verschiedene Werte.
Wie schon in Abschnitt 2.1 illustriert wurde, sind endliche zyklische Gruppen auch isomorph zu einer Gruppe von Drehungen. So kann $\mathbb{Z}/12\mathbb{Z}$ durch die Drehungen des Stundenzeigers einer Uhr veranschaulicht werden. Nach 12 Schritten befindet er sich wieder am Ausgangspunkt. Daraus erklärt sich der Name zyklisch.

Definition 3.3.12. Es sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Für $h \in G$ sei $H = \langle h \rangle$ die von h erzeugte Untergruppe. Diese besteht aus allen Potenzen von h: $H = \{\ldots, h^{-1}, e, h, h^2, \ldots\}$ und ist somit eine zyklische Gruppe. Die Mächtigkeit von $H = \langle h \rangle$ nennt man auch die Ordnung von h. Besteht h aus m verschiedenen Potenzen von h, so ist $H = \{e, h, \ldots, h^{m-1}\}$ und $h^m = e$. Dann ist H isomorph zu $(\mathbb{Z}/m\mathbb{Z}, +)$. Die Ordnung von h kann also auch so beschrieben werden: $|\langle h \rangle|$ ist der kleinste natürliche Exponent m, für den $h^m = e$ ist.

Beispiel 3.3.13. Es sei $G = ((\mathbb{Z}/7\mathbb{Z})^*, \cdot)$. Es sei H die von $h = 2 \mod 7$ erzeugte Untergruppe:

$$H = \{2^0 \mod 7 = 1 \mod 7, 2 \mod 7, 4 \mod 7\}.$$

Es ist $2^3 \mod 7 = 1 \mod 7$. Damit ist $|\langle 2 \mod 7 \rangle| = 3$.

Der folgende Satz gibt eine Übersicht über die Untergruppen von zyklischen Gruppen und auch über die Ordnung der von Gruppenelementen erzeugten Untergruppe.

Satz 3.3.14. *Es sei G eine zyklische Gruppe mit neutralem Element e. Jede Untergruppe von G ist ebenfalls zyklisch. Ist G unendlich, so ist jede Untergruppe $U \triangleleft G$ ebenfalls unendlich außer im Fall $U = \{e\}$.*
Ist $|G| = m \in \mathbb{N}$, so gibt es für jeden Teiler $d|m$ genau eine zyklische Untergruppe U von G mit $|U| = d$. Dies sind sämtliche Untergruppen von G.
Ist $G = \langle g \rangle$ und $|G| = m$, so ist

$$|\langle g^r \rangle| = \frac{m}{ggT(r, m)}.$$

Insbesondere ist genau dann $\langle g^r \rangle = G$, wenn $ggT(r, m) = 1$ ist.
Also hat G genau $\varphi(m)$ Erzeugende.

Wir haben schon in Beispiel 3.3.9 gesehen, daß die Gruppe $((\mathbb{Z}/7\mathbb{Z})^*, \cdot)$ zyklisch ist und von der Restklasse $3 \mod 7$ erzeugt wird. Man sagt auch: 3 ist eine Primitivwurzel $\mod 7$.
Auch der Begriff der Ordnung läßt sich übertragen: Die Tatsache, daß $3 \mod 7$ die Ordnung 6 hat, drückt man aus durch: $\mathrm{ord}_7\ 3 = 6$.
Beispiel 3.3.13 zeigt, daß $\mathrm{ord}_7\ 2 = 3$.

Definition 3.3.15. Es sei $m \in \mathbb{N}$ und $a \in \mathbb{Z}$. Unter $\mathrm{ord}_m\ a$ versteht man den kleinsten positiven Exponenten k, für den $a^k \equiv 1 \mod m$ ist. Eine ganze Zahl r heißt Primitivwurzel $\mod m$, wenn $\mathrm{ord}_m\ r = \varphi(m)$ ist.

Bemerkung 3.3.16. Es ist $\mathrm{ord}_m\ a$ also die Ordnung der von der Restklasse $a \mod m$ erzeugten Untergruppe von $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$.
Außerdem ist r genau dann Primitivwurzel $\mod m$, wenn die Restklasse $r \mod m$ die gesamte Gruppe $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ erzeugt, wenn also jede reduzierte Restklasse $\mod m$ als Potenz von $r \mod m$ geschrieben werden kann.

Das nächste Beispiel zeigt, daß nicht zu jedem Modul m eine Primitivwurzel existiert.

Beispiel 3.3.17. Es sei $m = 12$. Wir betrachten das reduzierte Restsystem $R = \{1, 5, 7, 11\}$. Es ist $\mathrm{ord}_{12}\ 1 = 1$ und $\mathrm{ord}_{12}\ 5 = \mathrm{ord}_{12}\ 7 = \mathrm{ord}_{12}\ 11 = 2$. Die von $1 \mod 12$ erzeugte Untergruppe von $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$ hat somit die Ordnung 1 und die von $5 \mod 12$, $7 \mod 12$ und $11 \mod 12$ erzeugten Untergruppen haben jeweils die Ordnung 2. Es gibt keine Restklasse, die die gesamte Gruppe $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$ erzeugt, also keine Restklasse der Ordnung 4, oder anders ausgedrückt: kein a mit $\mathrm{ord}_{12}\ a = 4$.
Die Gruppe $((\mathbb{Z}/12\mathbb{Z})^*, \cdot)$ ist nicht zyklisch.

Der nächste Satz gibt eine vollständige Auskunft über die Existenz von Primitivwurzeln.

Satz 3.3.18. *Eine Primitivwurzel* $r \mod m$ *existiert genau dann, wenn* $m = 1, 2, 4$ *oder wenn für eine Primzahl* $p > 2$ *und* $\gamma \in \mathbb{N}$ *gilt:* $m = p^\gamma$ *oder* $m = 2p^\gamma$*. In diesen Fällen ist die Gruppe* $((\mathbb{Z}/m\mathbb{Z})^*, \cdot)$ *zyklisch. Jede reduzierte Restklasse* $\mod m$ *ist eine Potenz von* $r \mod m$*.*

Abschließend betrachten wir die Frage, für welche Exponenten k die Kongruenz $a^k \equiv 1 \mod m$ gilt.

Satz 3.3.19. *Es sei* $m \in \mathbb{N}$*,* $a \in \mathbb{Z}$ *und* $ggT(a, m) = 1$*.*
Es gilt genau dann $a^k \equiv 1 \mod m$*, wenn* $\mathrm{ord}_m\ a \mid k$*.*
Insbesondere ist $\mathrm{ord}_m\ a$ *stets ein Teiler von* $\varphi(m)$*.*
Es ist genau dann $a^{k_1} \equiv a^{k_2} \mod m$*, wenn* $k_1 \equiv k_2 \mod ord_m a$*.*

Beweis. Es sei $k = q \cdot \mathrm{ord}_m\ a + r$ mit $0 \leq r < \mathrm{ord}_m\ a$. Dann ist $a^k = \left(a^{\mathrm{ord}_m\ a}\right)^q \cdot a^r \equiv a^r \mod m$.
Nach Definition 3.3.15 ist $a^r \equiv 1 \mod m \Leftrightarrow r = 0$.
Der Zusatz folgt wegen $a^{\varphi(m)} \equiv 1 \mod m$ (Satz 2.9.1, Euler). □

Kapitel 4

Polynomkongruenzen und Potenzreste

4.1 Polynomkongruenzen

Definition 4.1.1. Unter einer Polynomkongruenz verstehen wir eine Kongruenz der Form

$$P(x) \equiv 0 \mod m, \tag{$*$}$$

wobei P ein Polynom mit ganzzahligen Koeffizienten und m eine natürliche Zahl ist.
Bei der Betrachtung von $(*)$ können in $P(x)$ alle Koeffizienten, die durch m teilbar sind, weggelassen werden.

Beispiel 4.1.2. Die Kongruenz

$$15x^4 + 7x^3 + 5x^2 + 2x + 1 \equiv 0 \mod 3$$

ist äquivalent zu

$$7x^3 + 5x^2 + 2x + 1 \equiv 0 \mod 3,$$

da wegen $3|15$ gilt: $15x^4 \equiv 0 \mod 3$.

Dies gibt Anlaß zur folgenden

Definition 4.1.3. Hat $P(x)$ in $(*)$ die Form

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

mit $n \in \mathbb{N}$ und $a_n \not\equiv 0 \mod m$, so nennt man $(*)$ eine Polynomkongruenz vom Grad n.

In Abschnitt 2.6 haben wir die linearen Kongruenzen- in der Bezeichnungsweise von Definition 4.1.3 die Kongruenz vom Grad 1- betrachtet. Wir haben gesehen, daß deren Lösungsmenge sehr gut bekannt ist. Gut erforscht sind weiterhin die quadratischen Kongruenzen- Kongruenzen vom Grad 2- und die Theorie der Potenzreste: $x^n - a \equiv 0 \mod m$. Diese werden wir in den nächsten Abschnitten diskutieren. Über allgemeine Polynomkongruenzen sind nur wenige Tatsachen bekannt. Wir werden einige in diesem Abschnitt zusammenstellen.
Wie bei linearen Kongruenzen hängt die Tatsache, ob x eine Lösung von $P(x) \equiv 0 \mod m$ ist, nur von der Restklasse von $x \mod m$ ab.

Beispiel 4.1.4. Es sei

$$P(x) = x^3 - 2x^2 - x - 13.$$

Was sind die Lösungen von $P(x) \equiv 0 \mod 5$?
Wir berechnen die Werte von $P(x)$ für x aus dem absolut kleinsten Restsystem mod 5 und erhalten folgende Tabelle:

x	-2	-1	0	1	2
$P(x)$	-27	-15	-13	-15	-15

Die Lösungsmenge von $P(x) \equiv 0 \mod 5$ besteht also aus den folgenden drei Restklassen mod 5:

$$x \equiv 1 \mod 5, \quad x \equiv 2 \mod 5 \quad \text{und} \quad x \equiv 4 \mod 5.$$

Ist der Modul m einer Polynomkongruenz das Produkt von teilerfremden Moduln $m = m_1 \cdot m_2 \cdots m_r$, so ist die Kongruenz

$$P(x) \equiv 0 \mod m \tag{$*$}$$

äquivalent zum System der Kongruenzen

(∗∗)

$$\begin{aligned} P(x) &\equiv 0 \mod m_1 \\ &\vdots \quad\quad \vdots \\ P(x) &\equiv 0 \mod m_r. \end{aligned}$$

Die Lösungen der Kongruenz $(*)$ können aus den Lösungen des Systems $(**)$ mittels des Chinesischen Restsatzes mit dem Algorithmus von Satz 2.7.4 berechnet werden.

Beispiel 4.1.5. Es sei wieder $P(x) = x^3 - 2x^2 - x - 13$.
Man bestimme die Lösungsmenge von

$$P(x) \equiv 0 \mod 15. \tag{$*$}$$

Lösung:
Die Kongruenz $(*)$ ist äquivalent zu dem System

$$\begin{aligned} P(x) &\equiv 0 \mod 3 \quad (I) \\ P(x) &\equiv 0 \mod 5 \quad (II) \end{aligned}$$

Man überprüft leicht, daß die Lösungen von (I) aus den beiden Restklassen

$$x \equiv 1 \mod 3 \quad \text{und} \quad x \equiv 2 \mod 3$$

besteht.
In Beispiel 4.1.4 wurde gezeigt, daß die Lösungsmenge von (II) aus den drei Restklassen

$$x \equiv 1 \mod 5, \quad x \equiv 2 \mod 5 \quad \text{und} \quad x \equiv 4 \mod 5$$

besteht.
Man erhält sechs mögliche Kombinationen, die in folgender Tabelle dargestellt sind:

		Lösungen mod 5		
		1	2	4
Lösungen mod 3	1	1	7	4
	2	11	2	14

Die Lösungsmenge von $P(x) \equiv 0 \mod 15$ besteht also aus den sechs Restklassen

$$\begin{aligned} x &\equiv 1 \mod 15, \quad x \equiv 2 \mod 15, \quad x \equiv 4 \mod 15 \\ x &\equiv 7 \mod 15, \quad x \equiv 11 \mod 15, \quad x \equiv 14 \mod 15. \end{aligned}$$

Die in Beispiel 4.1.5 dargestellten Ideen können leicht zum Beweis des folgenden Satzes verwendet werden:

Satz 4.1.6. *Es sei $P(x)$ ein Polynom mit ganzzahligen Koeffizienten. Es sei $N(m)$ die Anzahl der Lösungen der Kongruenz $P(x) \equiv 0 \mod m$. Dann ist $N(m)$ eine multiplikative Funktion von m, d.h. für $m = m_1 \cdot m_2$ mit $ggT(m_1, m_2) = 1$ gilt:*

$$N(m) = N(m_1) \cdot N(m_2).$$

Wir schließen mit einem Resultat für Polynomkongruenzen nach Primzahlmoduln.

Satz 4.1.7. *Es sei p eine Primzahl und $P(x) = a_n x^n + a_{n-1} x^{n-1} \ldots + a_0$ mit $a_i \in \mathbb{Z}$ und $a_n \not\equiv 0 \mod p$. Dann besitzt die Kongruenz n- ten Grades*

$$P(x) \equiv 0 \mod p$$

höchstens n Lösungen.

Bemerkung 4.1.8. Wie Beispiel 4.1.5 zeigt, gilt diese Aussage nicht, falls der Modul keine Primzahl ist. Die Kongruenz dritten Grades

$$x^3 - 2x^2 - x - 13 \equiv 0 \mod 15$$

besitzt sechs Lösungen.

4.2 Potenzreste

Definition 4.2.1. Es sei $k, m \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $ggT(a, m) = 1$. Die Zahl a heißt dann k- ter Potenzrest modulo m, falls die Kongruenz

$$x^k \equiv a \mod m$$

lösbar ist, andernfalls ein k- ter Potenznichtrest.
Im Fall $k = 2$ spricht man von quadratischen Resten bzw. Nichtresten.

Beispiel 4.2.2. Es sei $k = 3$ und $m = 7$. Die 3. Potenzreste $\mod 7$ lassen sich durch Berechnen der dritten Potenzreste aller Elemente eines vollständigen Restsystems bestimmen. Wir erhalten folgende Tabelle:

$x \mod 7$	-3	-2	-1	0	1	2	3
$x^3 \mod 7$	1	-1	-1	0	1	1	-1

Die 3. Potenzreste $\mod 7$ bestehen also aus den Restklassen $1 \mod 7$ und $-1 \mod 7$.
Die Kongruenz

$$x^3 \equiv a \mod 7$$

besitzt für $a \equiv 1, -1 \mod 7$ jeweils drei Lösungen $\mod 7$ und sonst keine.

Die Theorie der Potenzreste $\mod m$ ist sehr übersichtlich, wenn m eine Primitivwurzel besitzt.

Satz 4.2.3. *Der Modul $m \in \mathbb{N}$ besitze eine Primitivwurzel. Es sei $k \in \mathbb{N}$ und $d = ggT(k, \varphi(m))$. Dann gibt es genau $\frac{\varphi(m)}{d}$ k- te Potenzreste $\mod m$. Ist $a \in \mathbb{Z}$ ein k- ter Potenzrest $\mod m$, d.h. ist $ggT(a, m) = 1$ und*

$$x^k \equiv a \mod m \qquad (*)$$

lösbar, so hat $(*)$ genau d Lösungen in $x \mod m$. Zudem ist $a \in \mathbb{Z}$ genau dann ein k- ter Potenzrest, wenn

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \mod m$$

ist.

Beweis. Es sei r eine Primitivwurzel $\mod m$. Für jedes Paar (x, a) von ganzen Zahlen mit $ggT(x, m) = ggT(a, m) = 1$ gibt es nach Satz 3.3.19 $\mod \varphi(m)$ eindeutig bestimmte Zahlen y, j mit

$$x \equiv r^y \mod m \quad \text{und} \quad a \equiv r^j \mod m.$$

Nach Satz 3.3.19 entsprechen die Lösungen $x \mod m$ von $(*)$ umkehrbar eindeutig den Lösungen $y \mod \varphi(m)$ der linearen Kongruenz

$$ky \equiv j \mod \varphi(m). \qquad (**)$$

Nach Satz 2.6.1 ist $(**)$ genau dann lösbar, wenn $d|j$ ist. Es gibt dann d Lösungen $\mod \varphi(m)$:

$$d|j \Leftrightarrow \varphi(m)|j\frac{\varphi(m)}{d} \leftrightarrow (r^j)^{\varphi(m)/d} \equiv 1 \mod m.$$

Die Lösbarkeit von $(*)$ ist also äquivalent zu $a^{\varphi(m)/d} \equiv 1 \mod m$. Es gibt $\frac{\varphi(m)}{d}$ Werte von j, welche die Bedingungen $d|j$ erfüllen. □

Wir formulieren den Spezialfall für $k = 2$, d.h. quadratische Reste, und $m = p > 2$ sei eine ungerade Primzahl.

Satz 4.2.4. *Es sei p eine ungerade Primzahl. Von den $p - 1$ Werten a mit $1 \leq a \leq p - 1$ sind genau $\frac{p-1}{2}$ quadratische Reste $\mod p$ (d.h. $x^2 \equiv a \mod p$ ist lösbar) und $\frac{p-1}{2}$ quadratische Nichtreste $\mod p$.*
Es gilt das Eulersche Kriterium:
a ist quadratischer Rest $\mod p \quad \Leftrightarrow \quad a^{p-1/2} \equiv 1 \mod p$.
a ist quadratischer Nichtrest $\mod p \quad \Leftrightarrow \quad a^{p-1/2} \equiv -1 \mod p$.

Im Falle $p = 3 \mod 4$ ergibt sich die Möglichkeit, einem quadratischen Rest $a \mod p$ die "Quadratwurzel" x, d.h. die Lösung von $x^2 \equiv a \mod p$ zu berechnen.

Satz 4.2.5. *Es sei $p \equiv 3 \mod 4$ eine Primzahl und a ein quadratischer Rest $\mod p$. Dann ist $x = a^{p+1/4}$ eine Lösung der Kongruenz $x^2 \equiv a \mod p$.*

Beweis. Es ist

$$x^2 = a^{p+1/2} = a \cdot a^{p-1/2} \equiv a \mod p,$$

da nach dem Eulerschen Kriterium $a^{p-1/2} \equiv 1 \mod p$ ist. □

Kapitel 5

Anwendungen in der Kryptologie, Primzahltests

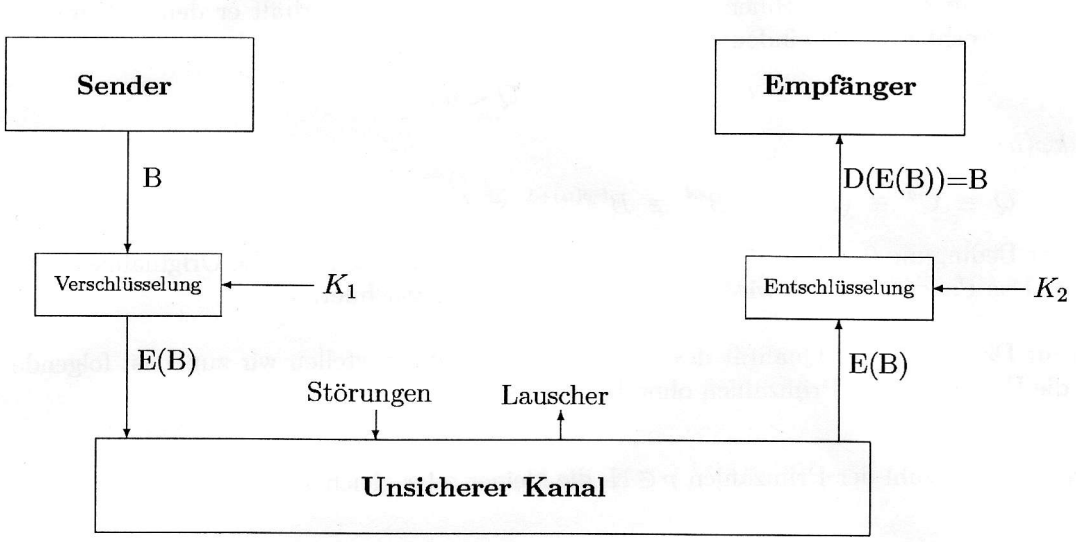
5.1 Public- Key- Codes, RSA- Verfahren

Der Gegenstand der Kryptologie ist die Übermittlung geheimer Botschaften unter Verwendung von Codes. Die Kryptologie besteht aus zwei Teilgebieten:

(i) In der Kryptographie wird der Entwurf von Geheimcodes untersucht.

(ii) In der Kryptoanalyse wird nach Methoden gesucht, diese zu knacken.

Bei der Übermittlung einer geheimen Nachricht wird zunächst eine Botschaft B in einen Geheimtext $E(B)$ umgeändert. Das Verfahren für die Umänderung bezeichnet man als Verschlüsselung E (von eng. "encryption"). Die verschlüsselte Botschaft wird dann an den Empfänger gesandt. Dieser benutzt ein Entschlüsselungsverfahren D (von engl. "decryption"), um dann die ursprüngliche Botschaft zurück zu gewinnen. Diese sogenannten Chiffrierverfahren sind öffentlich bekannt. Das Verschlüsselungsverfahren wird dabei meist durch einen Schlüssel K_1 gesteuert, die Entschlüsselung durch einen Schlüssel K_2. Die Übermittlung erfolgt also nach folgendem Schema:



Ziel der Chiffrierverfahren ist es, die Nachricht B vor dritten Personen geheimzuhalten und gegen Veränderungen bei der Übertragung zu schützen. Dazu ist es erforderlich, den Schlüssel K_2 vor eventuellen Lauschern geheimzuhalten. Bei den konventionellen Verfahren (den symmetrischen Chiffrierverfahren) ist es möglich, das Entschlüsselungsverfahren aus dem Verschlüsselungsverfahren zu gewinnen (meist sind diese sogar identisch, und es gilt: $K_1 = K_2$). Also war auch K_1 geheimzuhalten. In gewissen Umständen ist es jedoch wünschenswert, auf die Geheimhaltung von K_1 zu verzichten. Haben wir zum Beispiel ein Netzwerk von sehr vielen Teilnehmern, so ist es wünschenswert, daß jeder Teilnehmer T_i an jeden anderen´Teilnehmer T_j eine Botschaft schicken kann, ohne sich zunächst bei T_j nach dem Schlüssel zu erkundigen. Dazu veröffentlicht jeder Teilnehmer T_j seinen Schlüssel S_j für die Verschlüsselung in einer Art Telefonbuch. Will ein anderer Teilnehmer T_i eine Botschaft an T_j senden, so benutzt er dazu den Schlüssel S_j. Es muß also ein System gefunden werden, bei dem es unmöglich ist, den Schlüssel für die Entschlüsselung aus S_j zu berechnen. Einen solchen Code nennt man Public- Key- Code oder auch asymmetrisches Chiffrierverfahren. Wir werden das RSA- System (benannt nach Rivest, Shamir und Adleman, die es 1978 vorgeschlagen haben) betrachten.

Der öffentliche Schlüssel $S = (e, n)$ ist ein Zahlenpaar bestehend aus dem Exponenten $e \in \mathbb{N}$ und dem Modulus n, so daß $n = p \cdot q$ das Produkt zweier verschiedener Primzahlen ist und außerdem auch $ggT(e, \varphi(n)) = 1$ gilt. Während e und n allgemein zugänglich sind, ist die Faktorisierung $n = p \cdot q$ und auch $\varphi(n)$ nur dem Empfänger bekannt, dem der öffentliche Schlüssel gehört. Das Verfahren gilt als sicher, wenn p und q groß genug gewählt sind. Aktuelle Schlüssel (Stand: 2005) sind von der Größenordnung 2^{1024}.
Wir beschreiben nun das Verschlüsselungsverfahren: Jeder Buchstabe der Nachricht wird nach einem Standardverfahren in eine Ziffernfolge umgewandelt. Eine feste Anzahl dieser Ziffernfolgen werden aneinander gehängt, so daß sie eine Zahl $B < n$ bilden. Dabei soll B jedoch von derselben Größenordnung wie n sein, d.h. in etwa die gleiche Anzahl an Stellen besitzen. Ist die Botschaft länger, kann sie in Blöcke unterteilt werden. Der Absender berechnet dann die eindeutig bestimmte Zahl C mit $C \equiv B^e \mod n$ mit $0 < C < n$. Die Zahl C ist der Geheimtext, der an den Empfänger gesendet wird.
Wir kommen zur Beschreibung des nur dem Empfänger bekannten Entschlüsselungsverfahrens. Da der Empfänger die Faktorisierung $n = p \cdot q$ kennt, kann er auch $\varphi(n) = (p-1) \cdot (q-1)$ einfach ausrechnen. Da $ggT(e, \varphi(n)) = 1$ ist, kann der Empfänger ein $d > 0$ berechnen, so daß $ed \equiv 1 \mod \varphi(n)$ ist. Erhält er den Geheimtext $C \equiv B^e \mod n$, so berechnet er die eindeutig bestimmte Zahl Q mit $Q \equiv C^d \mod n$ mit $0 < Q < n$.
Dann ist $ed = k\varphi(n) + 1$ für ein $k \in \mathbb{N}_0$, also gilt

$$Q \equiv C^d \equiv (B^e)^d \equiv B^{ed} \equiv B^{k\varphi(n)+1} \equiv \left(B^{\varphi(n)}\right)^k \cdot B \equiv B \mod n.$$

Also ist wegen der Bedingung $0 < Q < n$ dann $Q = B$, d.h. der Empfänger hat die Originalnachricht zurückgewonnen. Das Paar $T = (d, n)$ wird als privater Schlüssel bezeichnet.

Bevor wir nun zur Diskussion der Qualität des RSA- Systems kommen, stellen wir zunächst folgende Tatsache über die Häufigkeit der Primzahlen ohne Beweis fest:

Definition 5.1.1. Für $x > 0$ sei $\pi(x)$ die Anzahl der Primzahlen $p \in \mathbb{N}$, die kleiner oder gleich x sind.

Es gilt:

Satz 5.1.2. *(Primzahlsatz)*

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1,$$

was auch geschrieben werden kann als

$$\pi(x) \sim \frac{x}{\log x}.$$

Die zweite Tatsache, die wir müssen wissen, und im nächsten Abschnitt diskutieren werden, ist, daß es sehr schnelle Primzahltests gibt. Die Anzahl der Rechenschritte für einen Primzahltest ist für eine Zahl der Größenordnung 2^k nur von der Größenordnung k. Wir kommen nun zur angekündigten Diskussion der Qualität des RSA- Systems:

(i) Ein öffentlicher Schlüssel (e, n) ist leicht zu konstruieren. Dazu wählt man irgendeine Zahl p der Größenordnung $\sim 2^k$ nach dem Zufallsprinzip. Die Wahrscheinlichkeit, daß p eine Primzahl ist, beträgt nach dem Primzahlsatz

$$\frac{\pi(2^k)}{2^k} \sim \frac{1}{\log(2^k)} \sim \frac{1}{k}.$$

Ein Rechner benötigt daher im Schnitt k Versuche, um eine Primzahl p der gewünschten Größenordnung zu finden. Der Teilnehmer T berechnet zwei verschiedene Primzahlen p und q auf diese Weise und veröffentlicht den Schlüssel (e, n) mit $n = p \cdot q$.

(ii) Verschlüsselung und Entschlüsselung können leicht mit Computern durchgeführt werden, es wird nur die Potenzierung mit einer natürlichen Zahl benötigt, die modulo n effiizient durch wiederholtes Quadrieren durchgeführt werden kann. Das Inverse d zu e kann mit dem Euklidischen Algorithmus berechnet werden, wenn p und q bekannt sind.

(iii) Es gibt zur Zeit kein Verfahren, das die Originalnachricht B aus $C \equiv B^e \mod n$ ohne Kenntnis von $\varphi(n)$ oder der Faktorisierung $n = p \cdot q$ (welche die Kenntnis von $\varphi(n) = (p-1) \cdot (q-1)$ impliziert) mit akzeptablem Aufwand ausrechnen kann.

5.2 Primzahltests

Aus dem kleinen Satz von Fermat wissen wir, daß für eine Primzahl n und beliebiges $a \in \mathbb{Z}$, das nicht durch p teilbar ist, die Kongruenz

$$a^n \equiv a \mod n$$

gilt.
Wenn wir umgekehrt eine Zahl a finden können, so daß $a^n \not\equiv a \mod n$ ist, so wissen wir, daß n zusammengesetzt ist.

Beispiel 5.2.1. Es sei $n = 63$ und $a = 2$. Es ist $2^6 = 64 \equiv 1 \mod n$. Es ist $1 < 2^l < 63$ für $1 \leq l \leq 5$ und daher ist $ord_{63}\, 2 = 6$. Also ist nach Satz 3.3.19

$$2^{63} \equiv 2^3 \equiv 8 \mod 63.$$

Insbesondere ist $a^n \not\equiv a \mod n$ für $a = 2$, also ist 63 zusammengesetzt.

Dies ist natürlich nicht der einfachste Weg, um zu zeigen, daß $n = 63$ zusammengesetzt ist, da die Faktoren 3 und 7 sehr schnell gefunden werden können. Doch ist die Methode für größere Werte von n die erfolgreichste. Zum Beispiel iet 1963 (Selfriedge und Hurwitz) bekannt, daß die Fermatzahl $F_{14} = 2^{2^{14}} + 1$ mit 4933 Dezimalstellen zusammengesetzt ist. Jedoch ist bis heute kein Primfaktor von F_{14} bekannt. Es wäre wünschenswert, wenn durch Überprüfen der Kongruenz auch gezeigt werden könnte, daß eine Zahl n auch ein Primzahl ist. Dies ist leider nicht möglich, da die Umkehrung des kleinen Satzes von Fermat falsch ist.

Beispiel 5.2.2. Es sei $n = 341 = 11 \cdot 31$. Durch den kleinen Satz von Fermat ist $2^{10} \equiv 1 \mod 11$, also $2^{340} \equiv 1 \mod 11$. Außerdem ist $2^{340} = \left(2^5\right)^{68} \equiv 1 \mod 31$, also folgt $2^{341} \equiv 2 \mod 341$, obwohl 341 keine Primzahl ist.

Definition 5.2.3. Es sei $a \in \mathbb{N}$. Ist n zusammengesetzt und $a^n \equiv a \mod n$, so heißt n eine Pseudo- Primzahl zur Basis a.

Pseudo- Primzahlen bzgl. einer Basis a sind viel seltener als Primzahlen. Insbesondere gibt es 455025512 Primzahlen $\leq 10^{10}$, aber nur 14884 Pseudo- Primzahlen $\leq 10^{10}$ zur Basis 2. Dennoch gibt es zu jeder Basis unendlich viele Pseudo- Primzahlen.

Satz 5.2.4. *Es gibt unendlich viele Pseudo- Primzahlen zur Basis 2.*

Es ist also nicht immer möglich, durch Überprüfen einer einzelnen Kongruenz $a^n \equiv a \mod n$ zu zeigen, daß n zusammengesetzt ist. Eine weitergehende Idee besteht darin, die Kongruenz für verschiedene Basen a zu testen. So ist $n = 341$ beispielsweise eine Pseudo- Primzahl zur Basis 2, jedoch keine Pseudo- Primzahl zur Basis 3, da $3^{341} \equiv 168 \not\equiv 3 \mod 341$ ist. Der Test mit der Basis $a = 3$ zeigt also, daß 341 zusammengesetzt ist. Es gibt jedoch auch Zahlen, die Pseudo- Primzahlen bzgl. jeder Basis sind.

Definition 5.2.5. Eine zusammengesetzte Zahl n, für die $a^{n-1} \equiv 1 \mod n$ für alle natürlichen Zahlen a mit $ggT(a, n) = 1$ gilt, heißt Carmichael- Zahl.

Es wurde 1992 von Alford, Granville und Pomerance gezeigt, daß es unendlich viele Carmichael- Zahlen gibt.

Satz 5.2.6. *Genau dann ist n eine Carmichael- Zahl, wenn $n = p_1 \cdot p_2 \cdots p_r$ mit $r \geq 3$ und paarweise verschiedenen ungeraden Primzahlen p_i ist, für die $(p_i - 1)|(n-1)$ für $i = 1, \ldots, r$ gilt.*

Wir kommen nun zur Beschreibung von Primzahltests:
Ist n eine Primzahl, so folgt aus der Kongruenz $a^{n-1} \equiv 1 \mod n$, daß $a^{\frac{n-1}{2}} \equiv \pm 1 \mod n$ ist. Man kann also versuchen zu zeigen, daß n zusammengesetzt ist, indem man diese Kongruenz überprüft.

Beispiel 5.2.7. Es sei $n = 561 = 3 \cdot 11 \cdot 17$. Nach Satz 5.2.6 ist n eine Carmichael- Zahl. Also ist $5^n \equiv 5 \mod n$. Es ist jedoch

$$5^{\frac{561-1}{2}} = 5^{280} \equiv 67 \mod 561.$$

Dies zeigt, daß $n = 561$ zusammengesetzt ist.

Definition 5.2.8. Es sei n eine natürliche Zahl mit $n - 1 = 2^s \cdot t$ mit $s \in \mathbb{N}_0$ und t eine ungerade natürliche Zahl. Wir sagen, n besteht den Test von Miller für die Basis a, wenn entweder $a^t \equiv 1 \mod n$ oder $a^{2^j t} \equiv -1 \mod n$ für ein j mit $0 \leq j \leq s - 1$ gilt.

Satz 5.2.9. *Ist n prim und a eine natürliche Zahl mit $n \not| a$, dann besteht n den Test von Miller für die Basis a.*

Beweis. Es sei $n - 1 = 2^s \cdot t$ mit $s \in \mathbb{N}_0$ und t eine ungerade natürliche Zahl. Wir setzen

$$x_k = a^{\frac{n-1}{2^k}} = a^{2^{s-k}t}$$

für $k = 0, 1, 2, \ldots, s$. Da n eine Primzahl ist, gilt nach Fermat $x_0 = a^{n-1} \equiv 1 \mod n$. Aus $x_1^2 = a^{n-1} \equiv 1 \mod n$ folgt $n|(x_1^2 - 1) = (x_1 + 1)(x_1 - 1)$ also $x_1 \equiv -1 \mod n$ oder $x_1 \equiv 1 \mod n$. Ist $x_1 \equiv 1 \mod n$, so gilt wegen $x_2^2 \equiv x_1 \equiv 1 \mod n$ nun $x_2 \equiv -1 \mod n$ oder $x_2 \equiv 1 \mod n$. Induktiv folgt aus $x_0 \equiv x_1 \equiv \ldots \equiv 1 \mod n$ dann $x_{k+1} \equiv -1 \mod n$ oder $x_{k+1} \equiv 1 \mod n$. Es gilt also entweder $x_k \equiv 1 \mod n$ für alle $k = 0, \ldots, s$ oder $x_k \equiv -1 \mod n$ für ein k. Damit besteht n den Test von Miller zur Basis a. □

Dies führt zu folgender Definition:

Definition 5.2.10. Ist n zusammengesetzt und besteht dennoch den Test von Miller für eine Basis a, so heißt n eine starke Pseudo- Primzahl zur Basis a.

Obwohl starke Pseudo- Primzahlen sehr selten sind, gibt es dennoch wiederum unendlich viele zu jeder Basis a. Es gibt jedoch kein Analogon der Carmichael- Zahlen zu starken Pseudo- Primzahlen: ist n zusammengesetzt, so kann man immer eine Basis a finden, für die n den Test von Miller nicht besteht, für die also n keine starke Pseudo- Primzahl ist.

Satz 5.2.11. *Es sei n eine ungerade zusammengesetzte Zahl. Dann besteht n den Test von Miller für höchstens $\frac{n-1}{4}$ Basen a mit $1 \leq a \leq n-1$.*

Beweis. Wir setzen $n-1 = 2^s \cdot t$ mit $s \in \mathbb{N}_0$ und t ungerade. Falls n eine starke Pseudo- Primzahl zur Basis a ist, gilt $a^{n-1} \equiv 1 \mod n$. Es sei

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \tag{1}$$

die Primfaktorzerlegung von n. Nach den Sätzen 3.3.18 und 4.2.3 hat die Kongruenz

$$x^{n-1} \equiv 1 \mod p_j^{e_j}$$

genau $N_j = ggT(n-1, p_j^{e_j-1}(p_j-1)) = ggT(n-1, p_j-1)$ Lösungen $\mod p_j^{e_j}$. Nach dem Chinesischen Restsatz gibt es daher genau

$$N = \prod_{j=1}^{r} ggT(n-1, p_j-1) = \prod_{j=1}^{r} N_j$$

inkongruente Lösungen von $x^{n-1} \equiv 1 \mod n$.

Fall 1:
In (1) sei $\alpha_k \geq 2$ für mindestens ein k. Es ist

$$\frac{p_k-1}{p_k^{\alpha_k}} = \frac{1}{p_k^{\alpha_k-1}} - \frac{1}{p_k^{\alpha_k}} \leq \frac{1}{3} - \frac{1}{3^2} \leq \frac{2}{9}.$$

Daher ist

$$N = \prod_{j=1}^{r} ggT(n-1, p_j-1) \leq \frac{2}{9} p_k^{e_k} \prod_{\substack{j=1 \\ j \neq k}}^{r} p_j \leq \frac{2}{9} n.$$

Da $\frac{2}{9}n \leq \frac{1}{4}(n-1)$ für $n \geq 9$ ist, folgt, daß $N \leq \frac{n-1}{4}$ ist. Es gibt also höchstens $\frac{n-1}{4}$ Zahlen a mit $1 \leq a \leq n$, für die n eine starke Pseudo- Primzahl zur Basis a ist.

Fall 2:
Es sei $n = p_1 \cdots p_r$ mit ungeraden und paarweise verschiedenen p_i. Es sei $p_i - 1 = 2^{s_i} t_i$ für $i = 1, 2, \ldots, r$. Wir numerieren die p_i so, daß $s_1 \leq s_2 \leq \ldots \leq s_r$ gilt und betrachten die Kongruenz

$$x^{2^j t} \equiv -1 \mod p_i. \tag{2}$$

Es sei $d_i = ggT(2^j t, p_i - 1) = ggT(2^j, 2^{s_i}) \cdot ggT(t, t_i)$. Nach Satz 3.3.18 ist -1 genau dann ein $(2^j t)$- ter Potenzrest $\mod p_i$, wenn

$$(-1)^{\frac{p_i-1}{d_i}} \equiv 1 \mod p_i$$

ist, also wenn $0 \leq j \leq s_i - 1$ ist. Die Kongruenz (2) hat dann $d_i = 2^j T_i$ Lösungen $\bmod p_i$ mit $T_i = ggT(t, t_i)$. Nach dem Chinesischen Restsatz gibt es $T_1 \cdot T_2 \cdots T_r$ inkongruente Lösungen von $x^t \equiv 1 \mod n$ und $2^{jr} T_1 \cdots T_r$ inkongruente Lösungen von $x^{2^j t} \equiv -1 \mod n$, wenn $0 \leq j \leq s_1 - 1$ ist. Es gibt daher insgesamt höchstens

$$T_1 \cdot T_2 \cdots T_r \cdot \left(1 + \sum_{j=1}^{s_1 - 1} 2^{jr}\right) = T_1 \cdot T_2 \cdots T_r \cdot \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right) \tag{3}$$

Zahlen a mit $1 \leq a \leq n-1$, für die n eine starke Pseudo- Primzahl ist. Wir zeigen im folgenden, daß der Ausdruck (3) nicht größer als $\frac{\varphi(n)}{4} \leq \frac{n-1}{4}$ ist. Wegen $T_1 \cdot T_2 \cdots T_r \leq t_1 \cdot t_2 \cdots t_r$ genügt es zu zeigen, daß

$$\frac{1 + \frac{2^{rs_1} - 1}{2^r - 1}}{2^{s_1 + s_2 + \ldots + s_r}} \leq \frac{1}{4} \tag{4}$$

ist.
Aus $s_1 \leq s_2 \leq \ldots \leq s_r$ folgt

$$\begin{aligned} \frac{1 + \frac{2^{rs_1} - 1}{2^r - 1}}{2^{s_1 + s_2 + \ldots + s_r}} &\leq \left(1 + \frac{2^{rs_1} - 1}{2^r - 1}\right) \cdot 2^{-rs_1} = \frac{1}{2^{rs_1}} + \frac{2^{rs_1} - 1}{2^{rs_1} \cdot (2^r - 1)} \\ &= \frac{1}{2^{rs_1}} + \frac{1}{2^r - 1} - \frac{1}{2^{rs_1}(2^r - 1)} = \frac{1}{2^r - 1} + \frac{2^r - 2}{2^{rs_1} \cdot (2^r - 1)} \\ &\leq \frac{1}{2^r - 1}. \end{aligned}$$

Die Ungleichung (4) ist also erfüllt, wenn $r \geq 3$ ist. Der verbleibende Fall ist $r = 2$, also $n = p_1 \cdot p_2$ mit $p_1 - 1 = 2^{s_1} t_1$ und $p_2 - 1 = 2^{s_2} t_2$ (ohne Einschränkung $s_1 \leq s_2$). Falls $s_1 < s_2$ ist, folgt (4): es gilt $s_1 \geq 1$ und $s_2 \geq 2$, denn $p_j - 1$ ist gerade, und damit

$$\begin{aligned} \frac{1 + \frac{2^{2s_1} - 1}{3}}{2^{s_1 + s_2}} &= 2^{-s_1 - s_2} + \frac{1}{3}\left(2^{s_1 - s_2} - 2^{-s_1 - s_2}\right) = \frac{2}{3} \cdot 2^{-s_1 - s_2} + \frac{1}{3} \cdot 2^{s_1 - s_2} \\ &\leq \frac{2}{3} \cdot 2^{-3} + \frac{1}{3} \cdot 2^{-1} = \frac{1}{12} + \frac{1}{6} = \frac{1}{4}. \end{aligned}$$

Falls $s_1 = s_2 = s$ ist, so haben wir $ggT(n-1, p_1 - 1) = 2^s T_1$ und $ggT(n-1, p_2 - 1) = 2^s T_2$. Es sei $p_1 > p_2$, dann ist $T_1 \neq t_1$. Wäre $T_1 = t_1$, also $(p_1 - 1) | (n-1)$, so wäre $n = p_1 \cdot p_2 \equiv p_2 \equiv 1 \mod p_1 - 1$. Das ist aber ein Widerspruch zu $p_1 > p_2$. Wegen $T_1 \neq t_1$ ist $T_1 \leq \frac{1}{3} t_1$. Analog folgt $T_2 \leq \frac{1}{3} t_2$, falls $p_1 < p_2$ ist. In beiden Fällen ist also $T_1 \cdot T_2 \leq \frac{1}{3} t_1 \cdot t_2$ mit

$$\left(1 + \frac{2^{2s_1} - 1}{3}\right) 2^{-s_1} \leq \frac{1}{2},$$

also

$$T_1 \cdot T_2 \cdot \left(1 + \frac{2^{2s_1} - 1}{3}\right) \leq t_1 \cdot t_2 \cdot \frac{1}{6} \cdot 2^{s_1} = \frac{1}{6} \varphi(n).$$

Damit ist (4) auch in diesem Fall bewiesen. □

Satz 5.2.11 liefert die Grundlage für den probabilistischen Primzahltest von Rabin. Dieser Test liefert keine vollständige Gewißheit, daß eine Zahl eine Primzahl ist, jedoch ist er für praktische Zwecke ausreichend. Seine Formulierung verwendet das Konzept der Wahrscheinlichkeiten.

Satz 5.2.12. *(Probabilistischer Primzahltest von Rabin)*
Es sei n eine natürliche Zahl. Man wähle nach dem Zufallsprinzip k natürliche Zahlen $< n$ und führe den Test von Miller mit n für jede dieser Basen durch. Wenn n zusammengesetzt ist, ist die Wahrscheinlichkeit, daß n alle k Tests besteht, kleiner als $\left(\frac{1}{4}\right)^k$.

Falls eine berühmte Vermutung aus der Zahlentherorie, die sogenannte verallgemeinerte Riemannsche Vermutung, richtig ist, gilt sogar: zu jeder zusammengesetzten Zahl n gibt es eine Basis a mit $a < 70\left(\frac{\log n}{\log 2}\right)^2$, so daß n den Test von Miller für die Basis a nicht besteht. Eine Konsequenz dieser Vermutung ist also die Gültigkeit des folgenden Primzahltests: Es sei n eine ungerade natürliche Zahl. Besteht n den Test von Miller für alle Basen $a < 70\left(\frac{\log n}{\log 2}\right)^2$, so ist n eine Primzahl.